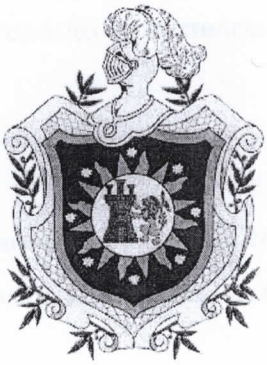
UNIVERSIDAD NACIONAL AUTONOMA DE NICARAGUA, MANAGUA

UNAN-MANAGUA

RECINTO UNIVERSITARIO "RUBEN DARIO"

FACULTAD DE CIENCIAS E INGENIERIA



TESIS PARA OPTAR AL TÍTULO DE:

MASTER EN COMPUTACIÓN

CON ÉNFASIS EN SISTEMAS DE INFORMACIÓN

Marco de referencia de seguridad de la información en el uso de los equipos de cómputo en la UNAN-Managua/FAREM-Estelí, aplicando la norma ISO 27001 en el periodo 2016

Autor: Lic. Manuel de Jesús Rivas Chavarría

Tutor: MSc. Danilo Avendaño López

Managua, 2016

Dedicatoria

A Dios

Antes que todo a Dios, el creador de todo lo existente, por permitirme día a día el milagro de la vida, por tener para mí un propósito de existencia.

A mi madre

A Rosario de Fátima Chavarría, maravillosa mujer, quien desde siempre ha sido mi punto de apoyo, con su fortaleza, dedicación y sacrificios logró formarme como una persona de bien.

A mis hijos

Christopher, Ramiro y Camila, mis tres regalos preciosos que Dios me ha concedido, por quienes tengo inspiración, tesón cada día, ustedes me permiten salir adelante alcanzando metas, las que se convierten en logros que son siempre suyas.

Agradecimiento

A la UNAN- Managua /FAREM- Estelí

Por permitirme la oportunidad de participar en esta maestría, y escalar en mi formación profesional.

A docentes de la FAREM- Estelí

Especial agradecimiento a mi amigo, el MSc. Nahúm Torrez, que me apoyo en todos los momentos que solicité su ayuda, y a todos los que en su momento me aconsejaron y brindaron palabras de aliento.

Tutor

Por el apoyo que me ha brindado durante todo este proceso al MSc. Danilo Avendaño, por sus sabios y oportunos consejos.

Resumen

La Seguridad de la Información tiene como fin la protección de la información y de los sistemas de la información del acceso, uso, divulgación, interrupción o destrucción no autorizada.

La seguridad es un concepto asociado a la certeza, falta de riesgo o contingencia. Podemos entender como seguridad un estado de cualquier sistema o tipo de información (informático o no) que nos indica que ese sistema o información está libre de peligro, daño o riesgo. Se entiende como peligro o daño todo aquello que pueda afectar a su funcionamiento directo o a los resultados que se obtienen.

La presente investigación es desarrollada en la Facultad Regional Multidisciplinaria FAREM-Estelí, recinto ubicado en el interior del país específicamente en la zona norte, perteneciente a la Universidad Nacional Autónoma de Nicaragua UNAN-Managua. La cual para desarrollar sus actividades ordinarias y extraordinarias hace uso de sistemas informáticos (equipos de cómputos, redes de comunicaciones de ordenadores, dispositivos de almacenamiento de información, entre otros). En dichos sistemas informático está presente la información, la que representa un importante y valioso activo.

El diseño metodológico que caracteriza esta investigación es mixto (cualitativo y cuantitativo) ya que se utilizaron las fortalezas de ambos tipos de indagación, haciendo una combinación de ellas y tratando de minimizar sus debilidades, esto con el fin de lograr un mayor entendimiento del fenómeno que se está estudiando. Al aplicar cada una de las herramientas de recolección de información sobre las vulnerabilidades a la que está expuesta la información a ser tomada por terceros, se logró una visión completa de las amenazas y riesgos de la exposición de este importante activo dando pautas para seleccionar de la ISO 27001 (norma internacional emitida por la Organización Internacional de Normalización que describe cómo gestionar la seguridad de la información en una

empresa), los dominios y controles que mejor se ajustan a las condiciones actuales de exposición de la información de la FAREM-Estelí.

A la vez se propone un marco de referencia de seguridad de la información en el uso de los equipos de cómputos en la UNAN-Managua/FAREM-Estelí, aplicando la norma ISO 27001, que en otras palabras es un documento de Declaración de Aplicabilidad (SoA por las siglas en inglés de Statement of Applicability).

Palabras claves

Información, Seguridad de la información, Sistemas de la información, riesgo, peligro, daño, activo, cualitativo, cuantitativo, vulnerabilidades, amenazas, ISO, marco de referencia, SoA.

Summary

The security of the information has as its main objective to protect the information of the systems, their use and divulging or authorized destruction. Security is a concept related to confidence, lack or risk or unexpectedness.

We can understand the concept of 'safety' as the state of any system of type of information (wether information system or not) that indicates that this system is out of danger, damage or risk. Damage and risk are understood as all factors that may negatively affect its functioning and its obtained results.

The present research is developed at the Facultad Regional Multidisciplinaria, (FAREM-Estelí), campus located in Northern-Nicaragua, which belongs to Universidad Nacional Autonoma de Nicaragua (UNAN-Managua). The university uses a variety of information systems in order to develop its ordinary and extraordinary activities (computing systems, communication networks, information storing devices, etc.). Such information systems are present in the information, which represents an important and valuable active.

The methodological design of this research is a mix methods design (qualitative and quantivative), since both designs have been implemented, combining them and trying to minize their weaknesses, this with the objective of achieving an understanding of the phenomenom under study. In order to apply one of the data collection tools about the vulnerabilities which the information is exposed to, a complete vision of the threats and the risk exposure was achived, in order to to select the ISO 27001 norm (international norm issued by the Normalization International Organization, which indicates how to manage the information security of a company), its domains and controls that best fit the current conditions of the information exposure of FAREM-Estelí.

At the same time, a reference standard for information security is proposed in the use of computing systems at UNAN-Managua/FAREM-Estelí, applying the norm ISO 27001, which in other words, is a document of Declaration of Applicability.

Key words

Vulnerability, Information, Safety, Information Systems, Risk, Danger, Damage, Active, ISO, reference standard.

Índice

Índice de Tablas

Índice de Figuras

I. Introducción

La información y los procesos que la apoyan, los sistemas y las redes, son bienes importantes de las entidades, por lo que requieren ser protegidos convenientemente frente a amenazas.

La información generalmente es procesada, intercambiada y conservada en redes de datos, equipos informáticos y soportes de almacenamiento, que son parte de lo que se conoce como sistemas informáticos. Los sistemas informáticos están sometidos a potenciales amenazas de seguridad de diversa índole, originadas tanto desde dentro de la propia organización, como desde fuera, procedentes de una amplia variedad de fuentes que ponen en peligro la disponibilidad, la integridad, la confidencialidad de la información (Carrasco, 2013).

Es posible disminuir el nivel de riesgo de forma significativa y con ello la materialización de las amenazas y la reducción del impacto sin necesidad de realizar elevadas inversiones ni contar con una gran estructura de personal.

Para ello se hace necesario conocer y gestionar de manera ordenada los riesgos a los que está sometido el sistema informático, considerar procedimientos adecuados y planificar e implantar los controles de seguridad que correspondan. Esta es la razón por lo que se planificó esta investigación, la cual se realizó desde el Departamento de Ciencias Tecnología y Salud de la UNAN-Managua/FAREM-Estelí.

La FAREM-Estelí posee dos áreas de trabajo en las cuales se utiliza equipo informático. Por un lado, en la parte institucional, todos los departamentos utilizan equipo; por otro lado, están los laboratorios de computación que también son utilizados por diversas personas. Por tanto, no está exenta a estos riesgos en ninguna de las áreas mencionadas, lo que hace necesario establecer mecanismos que con precisión indiquen qué está permitido y qué no está permitido manipular en los ordenadores.

Es importante destacar que por limitantes existentes entre los usuarios y la cantidad de equipos de cómputos de la FAREM-Estelí, muchos son multiusuarios; por lo que la información en ellos contenidos está expuesta, y por ende existe un alto grado de vulnerabilidad en el sentido de que la información llegue a manos de terceros.

Con ese fin, la investigación, que en su totalidad se realizó en el periodo 2016, tenía como primera parte la realización de un estudio para determinar el grado de vulnerabilidad de exposición de la información, mediante la metodología "Círculo de Deming también conocida como PDCA" (Planear, Hacer, Chechear, Actualizar).

Los resultados obtenidos sirvieron de base para la evaluación de los niveles de seguridad informática, y así visualizar un conjunto de controles, que incluyan marco de referencia, procesos, procedimientos, estructuras organizativas y funciones de hardware y software, los que deben ser establecidos, implementados, supervisados y mejorados cuando sea necesario para cumplir los objetivos específicos de seguridad de la institución.

El establecimiento de controles generales que se aplican por igual en todas las áreas y sistemas sin considerar su importancia y peculiaridades, producto como regla a la ausencia de un análisis de riesgos, conduce a que algunas áreas tengan un exceso de protección para las amenazas que enfrentan y otras no estén suficientemente protegidas.

El proponer un marco de referencia de seguridad de la información en el uso de los equipos de cómputo, en la FAREM Estelí, basadas en la norma ISO 27001 ayudó a establecer la forma más adecuada de tratar los aspectos de seguridad mediante la conjugación de los recursos humanos y técnicos, respaldados por medidas administrativas, que garanticen la instauración de controles efectivos para lograr el nivel de seguridad necesario.

El determinar controles generales y conformar un marco de referencia de seguridad es el objetivo de la segunda etapa de la investigación, que se realizó a partir de los resultados encontrados en la primera etapa, en la cual los riesgos están clasificados y priorizados para definir los controles a implementar.

En la tercera etapa, a partir de las conclusiones del estudio, se elaboró una propuesta a las autoridades de la FAREM-Estelí, a fin implementar los resultados de la investigación realizada.

II. Antecedentes

En muchos países, profesionales informáticos se capacitan en el desarrollo de buenas prácticas para la seguridad de la información en sus diferentes estados, puede ser en procesamiento, transición o almacenamiento.

En Nicaragua, un antecedente relacionado al tema de investigación de manera particular en la UNAN-Managua es el Sistema de Información Gerencial para el Instituto Nicaragüense de Fomento Cooperativo, basado en el dominio Planificación y Organización de COBIT 4.1 en el año 2011, realizado por el Licenciado Juan de Dios Bonilla, para optar al título de Maestro en Computación con Énfasis en Sistemas de Información. Dentro del mismo marco de la maestría antes mencionada se realizó otra tesis en febrero del año 2014 relacionada con la seguridad de la información, la que tiene por tema Políticas para las Tecnologías de la Información (TIC) en la dirección de informática de la Asociación Pueblos en Acción Comunitaria Aplicando COBIT 4.1, en el año 2013, realizada por el Licenciado Santiago Ramón Ríos Baca.

En la FAREM-Estelí, hasta ahora no se ha realizado un estudio relacionado directamente con la seguridad de la información, aunque es una institución que cuenta con un sistema de información (contenida en ordenadores en las diferentes oficinas y departamentos que conforma esta institución y una red de comunicación de equipos de cómputos con más de cien ordenadores) de considerables dimensiones.

III. Justificación

La información es un valioso activo del que depende el buen funcionamiento de una institución. Mantener su integridad, confidencialidad y disponibilidad es esencial para mantenerla protegida. Desafortunadamente, es relativamente fácil tener acceso a las herramientas que permiten a personas no autorizadas llegar hasta la información protegida, con poco esfuerzo y conocimientos, causando graves perjuicios.

La mayor parte de la información reside en equipos informáticos, soportes de almacenamiento y redes de datos, englobados dentro de lo que se conoce como sistemas de información. Estos sistemas de información están sujetos a riesgos y amenazas que pueden generarse desde dentro de la propia organización o desde el exterior. Por ejemplo, existen riesgos físicos como incendios, inundaciones, terremotos o vandalismo que pueden afectar la disponibilidad de nuestra información y recursos, haciendo inviable la operatividad de la institución si no estamos preparados para afrontarlos.

Por otra parte, se encuentran los riesgos lógicos relacionados con la propia tecnología y que aumentan día a día, hackers, robos de identidad, spam, virus, robos de información por nombrar algunos, pueden acabar con la confianza, imagen y prestigio que se ha construido a lo largo de muchos años.

Para proteger a la institución de todas estas amenazas, es necesario conocerlas y afrontarlas de una manera adecuada. Para ello debemos establecer unos procedimientos adecuados e implementar controles de seguridad basados en la evaluación de los riesgos y en una medición de su eficacia. Es necesario entonces establecer marcos de referencias, procedimientos, controles con objeto de disminuir los riesgos a los que la información está expuesta.

Sin embargo, ¿qué es lo que aporta a la institución la implantación de un marco de referencia de seguridad de la información para el uso de los ordenadores? ¿Cuáles son los beneficios que se observarán después de todo este proceso?

En primer lugar, se obtendrá una reducción de riesgos debido al establecimiento de un marco de referencia de seguridad de la información y seguimiento de controles sobre ellas. Con ello se logrará reducir las amenazas hasta alcanzar un nivel asumible por la institución. De este modo, si se produce una incidencia, los daños se minimizan.

En segundo lugar, se produce un ahorro de costes derivado de una racionalización de los recursos. Se eliminan las inversiones innecesarias e ineficientes como las producidas por desestimar o sobrestimar riesgos.

En tercer lugar, la seguridad se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la institución.

Por lo tanto, es de suma importancia que se cuente con un marco de referencia de seguridad de la información para proteger su integridad, disponibilidad y confidencialidad, reduciendo riesgos de que sea tomada por personas ajenas a la institución y que puedan usarla de manera mal intencionada.

IV. Planteamiento del problema

Como se ha mencionado antes, las instituciones corren riesgo de perder información contenida en sus ordenadores por no tomar las precauciones adecuadas de uso de los mismos, esto podría dañar su imagen, reputación, prestigio. De allí que sea necesario proteger la información (Carrasco, 2013).

La FAREM-Estelí no está exenta a estos riesgos, por lo que es necesario establecer mecanismos que con precisión indiquen qué está permitido y qué no está permitido manipular en los ordenadores.

Es importante destacar que por limitantes los equipos de cómputos de la FAREM-Estelí, muchos son multiusuarios; por lo que la información en ellos contenidos está expuesta y

por ende existe un alto grado de vulnerabilidad en que la información llegue a manos de terceros.

El estudio para determinar el grado de vulnerabilidad de exposición de la información a terceros en la FAREM-Estelí, se realizará en el periodo 2016.

4.1 Sistematización del problema

El presente estudio pretende dar respuesta a cuatro interrogantes principales:

a. ¿Cómo determinar un marco de referencia de seguridad de la información en el uso de los equipos de cómputo, en la UNAN-Managua/FAREM-Estelí, basadas en la norma ISO 27001, en el periodo 2016?

b. ¿Cuáles son las vulnerabilidades que exponen la información de los ordenadores a terceros en la Facultad Regional Multidisciplinaria FAREM, Estelí?

c. ¿Cuál es el marco de referencia de seguridad de la información más adecuado para el uso de los equipos de cómputos en la Facultad Regional Multidisciplinaria FAREM, Estelí?

d. ¿Cuáles son los beneficios que se observan después de todo este proceso?

e. ¿Qué es lo que aporta a la institución una propuesta de un marco de referencia de seguridad de la información para el uso de los ordenadores?

V. Sistema de objetivos

5.1 Objetivo general

Determinar un marco de referencia de seguridad de la información en el uso de los equipos de cómputo, en la UNAN-Managua/FAREM-Estelí, basadas en la norma ISO 27001, en el periodo 2016.

5.2 Objetivos específicos

1. Identificar las vulnerabilidades de la exposición de la información de los ordenadores a terceros.

2. Seleccionar los procedimientos de seguridad de la información de la norma ISO 27001 aplicables en la FAREM-Estelí.

3. Elaborar una propuesta de marco de referencia de seguridad de la información para el uso de los ordenadores, basadas en la norma ISO 27001.

4. Analizar la percepción de los usuarios acerca de la utilidad de la aplicación de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.

VI. Marco teórico

Revisando archivos investigativos desde fuentes bibliográficas e Internet se han integrado a este acápite teorías y conceptos que aportan sustancialmente al entendimiento pleno de terminologías que se usarán a lo largo de esta investigación, estructurándolo primeramente en marco teórico y posterior en marco conceptual.

6.1 Marco teórico

¿Qué es seguridad informática?

El término *seguridad informática* se define como un conjunto de métodos y técnicas destinados a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual participan además personas (Ramió, 2006).

Objetivo de la seguridad informática

La seguridad informática tiene como principal objetivo proteger el activo más importante que tiene la empresa que es su información de los riesgos a los que está expuesta (Carrasco, 2013). Para que la información sea considerada confiable para la organización ya que sus estrategias de negocio dependerán del almacenamiento, procesamiento y presentación de la misma, esta deberá cubrir los tres fundamentos básicos de seguridad para la información que son:

- Confidencialidad: Se define como la capacidad de proporcionar acceso a usuarios autorizados, y negarlo a no autorizados.
- Integridad: Se define como la capacidad de garantizar que una información o mensaje no han sido manipulados.
- Disponibilidad: Se define como la capacidad de acceder a información o utilizar un servicio siempre que lo necesitemos.

La seguridad informática se preocupa de que la información manejada por un computador no sea dañada o alterada, que esté disponible y en condiciones de ser procesada en cualquier momento y se mantenga confidencial.

Riesgos

Los riesgos se pueden definir como aquellas eventualidades que imposibilitan el cumplimiento de un objetivo y según la Organización Internacional por la Normalización (ISO, 2001) define riesgo tecnológico como la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes de un activo o un grupo de activos,

generándole pérdidas o daños. Podemos concluir que cualquier problema que afecte al total funcionamiento de la empresa es considerado un riesgo o amenaza para la entidad (Ramirez & Ortíz, 2011).

Evaluación de los riesgos

Proceso por el cual se identifican las vulnerabilidades de la seguridad. El objetivo general de evaluar los riesgos será identificar las causas de los riesgos potenciales, en toda la organización, a parte de ella o a los sistemas de información individuales, a componentes específicos de sistemas o servicios donde sea factible y cuantificarlos para que la Gerencia pueda tener información suficiente al respecto y optar por el diseño e implantación de los controles correspondientes a fin de minimizar los efectos de las causas de los riesgos (Ramirez & Ortíz, 2011).

Los pasos para realizar una valoración de riesgos se detallan a continuación:

Identificar los riesgos

En este paso se identifican los factores que introducen una amenaza en el entorno informático, existen formas de identificarlos como:

- **Cuestionarios de análisis de riesgos**: La herramienta clave en la identificación de riesgos son los cuestionarios los mismos que están diseñados para guiar al administrador de riesgos para descubrir amenazas a través de una serie de preguntas y en algunas instancias, este instrumento está diseñado para incluir riesgos asegurables e in-asegurables.
- **Listas de chequeo de exposiciones a riesgo**: Una segunda ayuda importante en la identificación de riesgos y una de las más comunes herramientas en el análisis de riesgos son las listas de chequeo, las cuales son simplemente unas listas de exposiciones a riesgo.

- **Listas de chequeo de políticas de seguridad**: Esta herramienta incluye un catálogo de varias políticas de seguridad que un negocio dado puede necesitar. El administrador de riesgos consulta las políticas recolectadas.

Análisis de los riesgos

Una vez se hayan identificado los riesgos, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución.

- **Ponderación de los Factores de riesgo**: Ponderar el factor de riesgo es darle un valor de importancia en términos porcentuales al mismo bajo los criterios de especialistas en el área informática que pueden identificar su impacto, teniendo en cuenta las posibilidades de que se puedan convertir en realidad.
- **Valoración del riesgo**: La valoración del riesgo envuelve la medición del potencial de las pérdidas y la probabilidad de la pérdida categorizando el orden de las prioridades.
    - ***Riesgo alto***: Todas las exposiciones a pérdida en las cuales la magnitud alcanza la paralización total de las actividades de la institución.
    - ***Riesgo medio***: Son exposiciones a pérdidas que no alcanzan la bancarrota, pero requieren una acción de la organización para continuar las operaciones.
    - ***Riesgo bajo***: Exposiciones a pérdidas que no causan un gran impacto.
    - ***Riesgo insignificante***: Es la exposición a pérdida que no provoca ningún daño.
- **Matriz descriptiva**: El objetivo de esta es la de asignar un valor a los recursos informáticos de acuerdo al impacto que el riesgo tenga sobre cada uno de ellos.
- **Matriz ponderada**: Esta matriz tiene como objetivo el determinar la prioridad de riesgo que tiene cada recurso informático mediante la obtención de un resultado determinado por la sumatoria de cada una de las multiplicaciones realizadas entre la ponderación de cada riesgo con la valoración de cada recurso informático.
- **Matriz categorizada**: El objetivo de esta matriz es la de definir la categoría del riesgo (Alto, Medio, Bajo e Insignificante) para cada recurso informático. Este valor

nos ayudará para definir las categorías de riesgo para nuestro análisis, dando a los valores altos la definición de "riesgo alto", a los valores medios "riesgo medio", a los valores bajos "riesgos bajos" y los valores insignificantes "riesgo insignificante".

Normas y/o Estándares Internacionales

Los estándares y normas son descripciones técnicas detalladas, elaboradas con el fin de garantizar la interoperabilidad entre elementos construidos independientemente, así como la capacidad de replicar un mismo elemento de manera sistemática.

Según la Organización Internacional para la Estandarización (ISO), uno de los principales organismos internacionales desarrolladores de estándares, la normalización es la actividad que tiene por objeto establecer, ante problemas reales o potenciales, disposiciones destinadas a usos comunes y repetidos, con el fin de obtener un nivel de ordenamiento óptimo en un contexto dado, que puede ser tecnológico, político o económico.

La familia de las ISO 27000

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad (desarrollados o en fase de desarrollo) que proporciona un marco para la gestión de la seguridad.

Contiene las mejores prácticas recomendadas en Seguridad de la información para desarrollar, implementar y mantener especificaciones para los Sistemas de Gestión de la

Seguridad de la Información (SGSI) utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

La seguridad de la información, según la ISO 27001

Se basa en la preservación de su confidencialidad, integridad y disponibilidad, así como la de los sistemas aplicados para su tratamiento, sustentada en el ciclo PDCA (conocido también como círculo de Deming).

Ciclo PDCA

El nombre del Ciclo PDCA (o Ciclo PHVA) viene de las siglas Planificar, Hacer, Verificar y Actuar, en inglés "Plan, Do, Check, Act". También es conocido como Ciclo de mejora continua o Círculo de Deming, por ser Edwards Deming su autor. Según Johnson (2005), ésta metodología describe los cuatro pasos esenciales que se deben llevar a cabo de forma sistemática para lograr la mejora continua, entendiendo como tal al mejoramiento continuado de la calidad (disminución de fallos, aumento de la eficacia y eficiencia, solución de problemas, previsión y eliminación de riesgos potenciales).

El círculo de Deming lo componen 4 etapas cíclicas, de forma que una vez acabada la etapa final se debe volver a la primera y repetir el ciclo de nuevo, de forma que las actividades son reevaluadas periódicamente para incorporar nuevas mejoras. La aplicación de esta metodología está enfocada principalmente para para ser usada en empresas y organizaciones.

La ISO 27001

Está estructurada en:

Dominios: Establecen 14 dominios o familias que agrupan controles destinados a la misma finalidad.

Objetivos de Control: Explican el objetivo al que darán solución los controles existentes.

Controles: 114 controles que identifican cada una de las acciones que deben realizarse para cumplir un objetivo.

Estructura general de la ISO 27001

Núm.	Nombre	Descripción / Justificación
1	Objeto y campo de aplicación	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
5	Políticas de seguridad de la información	
5.1	Directrices establecidas por la dirección para la seguridad de la información	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
6	Organización de la seguridad de la información	
6.1	Organización interna	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.

6.1.4	Contacto con grupos de interés especial	Control: Es conveniente mantener contactos apropiados con grupos de interés especial u otros foros y asociaciones profesionales especializadas en seguridad.
6.1.5	Seguridad de la información en la gestión de proyectos	Control: La seguridad de la información se debería tratar en la gestión de proyectos, independientemente del tipo de proyecto.
6.2	Dispositivos móviles y teletrabajo	Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles.
6.2.1	Política para dispositivos móviles	Control: Se deberían adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
6.2.2	Teletrabajo	Control: Se deberían implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
7	Seguridad de los recursos humanos	
7.1	Antes de asumir el empleo	Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.
7.1.1	Selección	Control: Las verificaciones de los antecedentes de todos los candidatos a un empleo se deberían llevar a cabo de acuerdo con las leyes, reglamentos y ética pertinentes, y deberían ser proporcionales a los requisitos de negocio, a la clasificación de la información a que se va a tener acceso, y a los riesgos percibidos.
7.1.2	Términos y condiciones del empleo	Control: Los acuerdos contractuales con empleados y contratistas, deberían establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
7.2	Durante la ejecución del empleo	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
7.3	Terminación o cambio de empleo	Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación del contrato.

7.3.1	Terminación o cambio de responsabilidades de empleo	Control: Las responsabilidades y los deberes de seguridad de la información que permanecen validos después de la terminación o cambio de contrato se deberían definir, comunicar al empleado o contratista y se deberían hacer cumplir.
8	Gestión de activos	
8.1	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.
8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.
8.1.3	Uso aceptable de los activos	Control: Se deberían identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de partes externas deberían devolver todos los activos de la organización que se encuentren a su cargo, al terminar su empleo, contrato o acuerdo.
8.2	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
8.2.1	Clasificación de la información	Control: La información se debería clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.
8.2.2	Etiquetado de la información	Control: Se debería desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.2.3	Manejo de activos	Control: Se deberían desarrollar e implementar procedimientos para el manejo de activos, de acuerdo con el esquema de clasificación de información adoptado por la organización.
8.3.1	Gestión de medios removibles	Control: Se deberían implementar procedimientos para la gestión de medios removibles, de acuerdo con el esquema de clasificación adoptado por la organización.
8.3.2	Disposición de los medios	Control: Se debería disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
8.3.3	Transferencia de medios físicos	Control: Los medios que contienen información se deberían proteger contra acceso no autorizado, uso indebido o corrupción durante el transporte.
9	Control de acceso	
9.1	Requisitos del negocio para control de acceso	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.

9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
9.1.2	Política sobre el uso de los servicios de red	Control: Solo se debería permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.
9.2	Gestión de acceso de usuarios	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de la información secreta se debería controlar por medio de un proceso de gestión formal.
9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deberían revisar los derechos de acceso de los usuarios, a intervalos regulares.
9.2.6	Retiro o ajuste de los derechos de acceso	Control: Los derechos de acceso de todos los empleados y de usuarios externos a la información y a las instalaciones de procesamiento de información se deberían retirar al terminar su empleo, contrato o acuerdo, o se deberían ajustar cuando se hagan cambios.
9.3	Responsabilidades de los usuarios	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
9.3.1	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
9.4	Control de acceso a sistemas y aplicaciones	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
9.4.4	Uso de programas utilitarios privilegiados	Control: Se debería restringir y controlar estrictamente el uso de programas utilitarios que pudieran tener capacidad de anular el sistema y los controles de las aplicaciones.

9.4.5	Control de acceso a códigos fuente de programas	Control: Se debería restringir el acceso a los códigos fuente de los programas.
10	Criptografía	
10.1	Controles criptográficos	Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, la autenticidad y/o la integridad de la información.
10.1.1	Política sobre el uso de controles criptográficos	Control: Se debería desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
10.1.2	Gestión de llaves	Control: Se debería desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
11	Seguridad física y del entorno	
11.1	Áreas seguras	Objetivo: Prevenir el acceso físico no autorizado, el daño y la interferencia a la información y a las instalaciones de procesamiento de información de la organización.
11.1.1	Perímetro de seguridad física	Control: Se deberían definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información sensible o critica, e instalaciones de manejo de información.
11.1.2	Controles físicos de entrada	Control: Las áreas seguras se deberían proteger mediante controles de entrada apropiados para asegurar que solamente se permite el acceso a personal autorizado.
11.1.3	Seguridad de oficinas, recintos e instalaciones	Control: Se debería diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
11.1.4	Protección contra amenazas externas y ambientales	Control: Se debería diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
11.1.5	Trabajo en áreas seguras	Control: Se deberían diseñar y aplicar procedimientos para trabajo en áreas seguras.
11.1.6	Áreas de despacho y carga	Control: Se deberían controlar los puntos de acceso tales como áreas de despacho y de carga, y otros puntos en donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
11.2	Equipos	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.
11.2.1	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
11.2.2	Servicios de suministro	Control: Los equipos se deberían proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministro.
11.2.3	Seguridad del cableado	Control: El cableado de potencia y de telecomunicaciones que porta datos o soporta servicios de información debería estar protegido contra interceptación, interferencia o daño.

11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
11.2.5	Retiro de activos	Control: Los equipos, información o software no se deberían retirar de su sitio sin autorización previa.
11.2.6	Seguridad de equipos y activos fuera de las instalaciones	Control: Se deberían aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta los diferentes riesgos de trabajar fuera de dichas instalaciones.
11.2.7	Disposición segura o reutilización de equipos	Control: Se deberían verificar todos los elementos de equipos que contengan medios de almacenamiento, para asegurar que cualquier dato sensible o software con licencia haya sido retirado o sobrescrito en forma segura antes de su disposición o reutilización.
11.2.8	Equipos de usuario desatendidos	Control: Los usuarios deberían asegurarse de que a los equipos desatendidos se les dé protección apropiada.
11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
12	Seguridad de las operaciones	
12.1	Procedimientos operacionales y responsabilidades	Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.
12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deberían documentar y poner a disposición de todos los usuarios que los necesiten.
12.1.2	Gestión de cambios	Control: Se deberían controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.
12.1.3	Gestión de capacidad	Control: Para asegurar el desempeño requerido del sistema se debería hacer seguimiento al uso de los recursos, hacer los ajustes, y hacer proyecciones de los requisitos sobre la capacidad futura.
12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deberían separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
12.2	Protección contra códigos maliciosos	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
12.2.1	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
12.3	Copias de respaldo	Objetivo: Proteger contra la perdida de datos.

12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
12.4	Registro y seguimiento	Objetivo: Registrar eventos y generar evidencia.
12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
12.4.3	Registros del administrador y del operador	Control: Las actividades del administrador y del operador del sistema se deberían registrar, y los registros se deberían proteger y revisar con regularidad.
12.4.4	sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinentes dentro de una organización o ámbito de seguridad se deberían sincronizar con una única fuente de referencia de tiempo.
12.5	Control de software operacional	Objetivo: Asegurar la integridad de los sistemas operacionales.
12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
12.6	Gestión de la vulnerabilidad técnica	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
12.7	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.
12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
13	Seguridad de las comunicaciones	
13.1	Gestión de la seguridad de las redes	Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.
13.1.1	Controles de redes	Control: Las redes se deberían gestionar y controlar para proteger la información en sistemas y aplicaciones.
13.1.2	Seguridad de los servicios de red	Control: Se deberían identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicios de red,

		ya sea que los servicios se presten internamente o se contraten externamente.
13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deberían separar en las redes.
13.2	Transferencia de información	Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.
13.2.1	Políticas y procedimientos de transferencia de información	Control: Se debería contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicación.
13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deberían tener en cuenta la transferencia segura de información del negocio entre la organización y las partes externas.
13.2.3	Mensajería electrónica	Control: Se debería proteger adecuadamente la información incluida en la mensajería electrónica.
13.2.4	*Acuerdos de* confidencialidad o de no divulgación	*Control: Se deberían identificar, revisar regularmente* y documentar los requisitos para los acuerdos de confidencialidad o no divulgación que reflejen las necesidades de la organización para la protección de la información.
14	Adquisición, desarrollo y mantenimientos de sistemas	
14.1.1	Requisitos de seguridad de los sistemas de información	Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios en redes públicas.
14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deberían incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.
14.1.2	Seguridad de servicios de las aplicaciones en redes publicas	Control: La información involucrada en los servicios de aplicaciones que pasan sobre redes públicas se debería proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.
14.1.3	Protección de transacciones de los servicios de las aplicaciones	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se debería proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.
14.2	Seguridad en los procesos de desarrollo y soporte	Objetivo: Asegurar de que la seguridad de la información esté diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.
14.2.1	Política de desarrollo seguro	Control: Se deberían establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos que se dan dentro de la organización.
14.2.2	Procedimientos de control de cambios en sistemas	Control: Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deberían controlar mediante el uso de procedimientos formales de control de cambios.

14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Control: Cuando se cambian las plataformas de operación, se deberían revisar las aplicaciones críticas del negocio, y ponerlas a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.
14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se deberían desalentar las modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, y todos los cambios se deberían controlar estrictamente.
14.2.5	Principios de construcción de sistemas seguros	Control: Se deberían establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
14.2.6	Ambiente de desarrollo seguro	Control: Las organizaciones deberían establecer y proteger adecuadamente los ambientes de desarrollo seguros para las tareas de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
14.2.7	Desarrollo contratado externamente	Control: La organización debería supervisar y hacer seguimiento de la actividad de desarrollo de sistemas contratados externamente.
14.2.8	Pruebas de seguridad de sistemas	Control: Durante el desarrollo se deberían llevar a cabo pruebas de funcionalidad de la seguridad.
14.2.9	Prueba de aceptación de sistemas	Control: Para los sistemas de información nuevos, actualizaciones y nuevas versiones, se deberían establecer programas de prueba para aceptación y criterios de aceptación relacionados.
14.3	Datos de prueba	Objetivo: Asegurar la protección de los datos usados para pruebas.
14.3.1	Protección de datos de prueba	Control:Los datos de ensayo se deberían seleccionar, proteger y controlar cuidadosamente.
15	Relación con los proveedores	
15.1	Seguridad de la información en las relaciones con los proveedores	Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.
15.1.1	Política de seguridad de la información para las relaciones con proveedores	Control: Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deberían acordar con estos y se deberían documentar.
15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores	Control: Se deberían establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información de la organización.

15.1.3	Cadena de suministro de tecnología de información y comunicación	Control: Los acuerdos con proveedores deberían incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología de información y comunicación.
15.2	Gestión de la prestación de servicios con los proveedores	Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores.
15.2.1	Seguimiento y revisión de los servicios de los proveedores	Las organizaciones deberían hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.
15.2.2	Gestión de cambios en los servicios de proveedores	Control: Se deberían gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados, y la revaloración de los riesgos.
16	Gestión de incidentes de seguridad de la información	
16.1	Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
16.1.1	Responsabilidad y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.

16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	
17.1	Continuidad de seguridad de la información	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
17.2	Redundancias	Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.
17.2.1	Disponibilidad de instalaciones de procesamiento de información.	Control: Las instalaciones de procesamiento de información se deberían implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
18	Cumplimiento	

18.1	Cumplimiento de requisitos legales y contractuales	Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.
18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Control: Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, y el enfoque de la organización para cumplirlos, se deberían identificar y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
18.1.2	Derechos de propiedad intelectual	Control: Se deberían implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
18.1.3	Protección de registros	Control: Los registros se deberían proteger contra perdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación, contractuales y de negocio.
18.1.4	Privacidad y protección de datos personales	Control: Cuando sea aplicable, se deberían asegurar la privacidad y la protección de la información de datos personales, como se exige en la legislación y la reglamentación pertinentes.
18.1.5	Reglamentación de controles criptográficos	Control: Se deberían usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
18.2	Revisiones de seguridad de la información	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.
18.2.2	Cumplimiento con las políticas y normas de seguridad	Control: Los directores deberían revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.

18.2.3	Revisión del cumplimiento técnico	Control: Los sistemas de información se deberían revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

Tabla No.1: Controles del Anexo A del estándar ISO/IEC 27001 y dominios a los que pertenece

Facultad Regional Multidisciplinaria (FAREM-Estelí)

La Facultad Regional Multidisciplinaria Estelí (FAREM-Estelí) de la Universidad Nacional Autónoma de Nicaragua, Managua (UNAN-Managua) es una institución pública de educación superior con incidencia en la región centro-norte del país. En el contexto de su misión, la FAREM-Estelí forma profesionales en distintas áreas del conocimiento, promueve la investigación científica y la extensión universitaria, en función de aportar al desarrollo local, regional y nacional.

Actualmente presenta una oferta académica de 23 carreras con grado de licenciatura y 6 carreras con grado de ingeniería, distribuidas en tres departamentos académicos: Ciencias de la Educación y Humanidades, Ciencias Económicas y Administrativas; Ciencias, Tecnología y Salud.

La población estudiantil es de 3,499. La planta docente está constituida por 63 profesores de contratación indefinida y 95 profesores de contratación parcial. El personal administrativo está compuesto por 79 trabajadores.

Misión:

Formar profesionales integrales dotados de valores fundamentales, de conocimientos científico-técnicos y competencias necesarias para ser agentes de cambio capaces de incidir positivamente en el desarrollo de la región segoviana en particular y del país en general, todo lo anterior a través del conocimiento eficaz y eficiente de las funciones académico-docente, investigativa, de extensión, proyección socio cultural y formación permanente.

Institución de estudios superiores de mayor prestigio en el norte del país, de carácter público, comprometida con los sectores populares, con su quehacer permanente centrado en la formación de profesionales altamente calificados y competentes en lo científico, técnico, humanístico, para que aporten significativamente sus conocimientos, su ejemplaridad, su liderazgo y demás capacidades, el desarrollo social, cultural, económico y político del país.

6.2 Marco conceptual

- **Información**: Según la Real Académica Española (2008), se define como acción y efecto de informar, comunicación o adquisición de conocimientos que permiten ampliar o precisar los que se poseen sobre una materia determinada, o conocimientos así comunicados o adquiridos.

  Conjunto de datos propios que se gestionan y mensajes que se intercambian personas y/o máquinas dentro de una organización. La información da las pruebas de la calidad y circunstancias en las que se encuentra la empresa.

- **Factores de riesgos**: Manifestaciones o características medibles u observables de un proceso que indican la presencia de riesgo atienden a aumentar la exposición, pueden ser interna o externa a la entidad (Carrasco, 2013).

- **Impacto**: Es la medición y valoración del daño que podría producir a la institución un incidente de seguridad. La valoración global se obtendrá sumando el coste de reposición de los daños tangibles y la estimación, siempre subjetiva, de los daños intangibles (Carrasco, 2013).

- **Amenaza**: Cualquier evento que pueda provocar daño a la información, produciendo a la empresa pérdidas materiales, financieras o de otro tipo.

- **Riesgo**: Proximidad o posibilidad de un daño, peligro, etc. Cada uno delos imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

- **Incidente de seguridad**: Cualquier evento que tenga, o pueda tener, como resultado la interrupción de los servicios suministrados por un Sistema de Información y/o pérdidas físicas, de activos o financieras. En otras palabras la materialización de una amenaza.

- **Seguridad informática**: Abarca los conceptos de seguridad física y seguridad lógica. Se le puede dividir como Área General y como Área Específica (seguridad de Explotación, seguridad de las Aplicaciones, etc.).

- **Seguridad física**: Consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención ante amenazas a los recursos e información confidencial que puedan interrumpir procesamiento de información. Se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

- **Seguridad lógica**: Consiste en la aplicación de barreras y procedimientos para mantener la seguridad en el uso de software, la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información. Se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

- **Vulnerabilidad**: Cualquier debilidad en los Sistemas de Información que pueda permitir a las amenazas causarles daños y producir pérdidas.

- Marco de referencia: Es el documento que establece los lineamientos, normativas, reglamentos, controles y procedimientos que se emplearan en un determinado contexto (Carrasco, 2013).

VII. Hipótesis

El determinar un marco de referencia de seguridad de la información en el uso de los equipos de cómputo en la UNAN-Managua/FAREM-Estelí, basadas en la norma ISO 27001, disminuirá el riesgo que la información sea usada por terceros.

VIII. Diseño metodológico

8.1 Enfoque y tipo de investigación

El enfoque de esta investigación será mixto (cualitativo y cuantitativo). Según Sampieri, Collado y Lucio (2010), la meta de la investigación mixta no es remplazar a la investigación cuantitativa ni a la investigación cualitativa, sino utilizar las fortalezas de ambos tipos de indagación combinándolas y tratando de minimizar sus debilidades potenciales.

Los métodos mixtos representan un conjunto de procesos sistemáticos, empíricos y críticos de investigación e implican la recolección y el análisis de datos cuantitativos y cualitativos, así como su integración y discusión conjunta, para realizar inferencias producto de toda la información recabada y lograr un mayor entendimiento del fenómeno bajo estudio (Sampieri, Collado & Lucio, 2010).

La investigación tendrá enfoque cuantitativo porque consiste en utilizar la recolección y el análisis de datos para contestar preguntas de investigación y probar hipótesis establecidas previamente, y confía en la medición numérica, el conteo y frecuentemente en el uso de la estadística para establecer con exactitud patrones de comportamiento en una población. Así mismo, la investigación será cualitativa la cual consiste en utilizar la recolección de datos

sin medición numérica para descubrir o afinar preguntas de investigación en el proceso de interpretación.

Además, será una investigación aplicada y descriptiva. Aplicada porque se utilizarán los conocimientos en la práctica y descriptiva porque se describirán detalladamente cada una de las etapas de la investigación según los objetivos específicos, también porque se medirá el grado de vulnerabilidad de la información a ser tomada por terceras personas.

8.2 Universo: Para este trabajo de investigación se tomará como universo la Facultad Regional Multidisciplinaria de Estelí (FAREM- Estelí). Con un total de 105 equipos de cómputos, equivalentes al 100% del universo.

8.3 Población: Los ordenadores de los departamentos académicos y oficinas de pedagogía y matemática, contabilidad de la FAREM-Estelí. Con un total de 33 equipos de cómputos, equivalentes al 31% del universo.

8.4 Muestra: Los equipos de cómputo de las tres secretarias de los departamentos académicos (1 por cada uno de ellos) y diez usuarios finales de las oficinas de pedagogía y matemática (5 por cada oficina) y la oficina de contabilidad (4 equipos de cómputo), para un total de 17 equipos de cómputos, equivalentes al 51% de la población.

8.5. Muestreo intencional: Este tipo de muestreo se caracteriza por un esfuerzo deliberado de obtener muestras "representativas" mediante la inclusión en la muestra de grupos típicos. Selecciona directa e intencionadamente los individuos de la población. El caso más frecuente de este procedimiento el utilizar como muestra los individuos a los que se tiene fácil acceso.

8.6 Operacionalización de variables

Objetivos	Variable/ Categoría	Definición conceptual	Dimensiones	Indicadores/ subcategorías	Técnicas e instrumentos
Identificar las vulnerabilidades de la exposición de la información de los ordenadores a terceros.	Vulnerabilidades de la exposición de la información de los ordenadores	En seguridad informática, la palabra vulnerabilidad hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones.	Vulnerabilidades por negligencia del usuario. Vulnerabilidades técnicas.	- Falta de sigilo con la palabra secreta. - Utilizar contraseñas fáciles de descubrir. - **Condiciones de los ordenadores en cuanto a:** Restricciones de acceso a la información o acceso sin contraseña. - Crear contraseñas con un débil patrón.	Entrevista Encuesta Diagnóstico técnico

Objetivos	Variable/ Categoría	Definición conceptual	Dimensiones	Indicadores/ subcategorías	Técnicas e instrumentos
Seleccionar los procedimientos de seguridad de la información de la norma ISO 27001 aplicables en la FAREM Estelí.	Norma ISO 27001	Conjunto de Dominios, objetivos de control y controles de seguridad que proporciona crear un marco para la gestión de la seguridad.	Dominios Objetivos de controles Controles	Selección de Dominios, objetivos de control y controles	ISO 27001
Definir una propuesta de marco de referencia de seguridad de la información para el uso de los ordenadores, basadas en la norma ISO 27001.	Marco de referencia de seguridad de la información en el uso de los equipos de cómputo, basadas en la norma ISO 27001.	Conjunto de normativas, reglamentos, controles y procedimientos en el uso de los equipos de cómputo, basadas en la norma ISO 27001.	Normativas Reglamentos Controles Procedimientos Sanciones	- **Normas para el uso de los ordenadores:** -Uso de una contraseña por el usuario -Instalación de programas -Almacenamiento de información -Descarga de archivos - **Normas de acceso físico al lugar de los ordenadores:** Restricciones de acceso a las	Entrevista Encuesta Diagnóstico técnico

Objetivos	Variable/ Categoría	Definición conceptual	Dimensiones	Indicadores/ subcategorías	Técnicas e instrumentos
				oficinas a personal no autorizado.	
Conocer la percepción de los usuarios acerca de la utilidad de la aplicación de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.	Percepción de los usuarios acerca de la utilidad de la aplicación de un marco de referencia para la protección de la información contenida en los equipos de cómputo.	Apreciaciones de los usuarios a cerca de los beneficios de la existencia de un marco de control de seguridad de la información en el uso de los equipos de cómputo.	Opiniones favorables. Opiniones desfavorables.	De acuerdo En desacuerdo	Encuesta

Tabla No.2: Operacionalización de variables.

8.7. Métodos e instrumentos para la recolección de datos

Definido el tipo de estudio en esta investigación, el universo, población, muestra y muestreo adecuada al problema de estudio, fue necesario determinar los métodos e instrumentos a utilizar en la recolección de datos para el conocimiento de la situación actual del problema en estudio, encontrándose como métodos aplicables entrevista, encuesta, diagnóstico técnico.

8.7.1 La entrevista. Es una de las técnicas más utilizadas en la investigación. Mediante ésta una persona (entrevistador) solicita información a otra (entrevistado). En esta técnica, el investigador debe tener excelentes capacidades de escuchar y captar información (Sampieri, Collado & Lucio, 2010).

Se realizó una entrevista semi- estructurada al personal técnico a cargo del soporte de hardware y software de los ordenadores de la FAREM-Estelí. En éste tipo de pregunta, el entrevistador lleva una pauta o guía con los temas a cubrir, los términos a usar y el orden de las preguntas. Sin embargo, los temas frecuentemente cambian en el curso de la entrevista, y surgen nuevas preguntas en función de lo que dice el entrevistado. A diferencia de los cuestionarios, se basan en preguntas abiertas adaptando flexibilidad (Sampieri, Collado & Lucio, 2010). Mediante ésta, se pretende obtener la información cualitativa de este estudio mixto.

8.7.2 La encuesta. Consiste en una investigación realizada sobre una muestra de sujetos, representativa de un colectivo más amplio que se lleva a cabo en el contexto de la vida cotidiana, utilizando procedimientos estandarizados de interrogación con el fin de conseguir mediciones cuantitativas sobre una gran cantidad de características objetivas y subjetivas de la población (Sampieri, Collado & Lucio, 2010).

Se realizó la encuesta a los usuarios finales de los ordenadores de la FAREM-Estelí.

8.7.3 Diagnostico técnico. Se realizaron visitas in situ a las oficinas de los departamentos de Ciencia tecnología y salud, empresariales y administrativas, educación y humanidades, también a las oficinas de pedagogía, matemática y contabilidad. Para tal caso se realizó una guía de observación la que permitió lograr evidencias de las condiciones actuales de los equipos de cómputos, dichas pruebas están soportadas por capturas de pantallas que se expresan por mismas.

8.8. Procedimiento para la recolección de la información

Principalmente se realizaron visitas a las oficinas de soporte técnico y de los usuarios finales de los ordenadores. Las entrevistas se aplicaron a los responsables de soporte técnico; a los dos miembros que forman este equipo. Para realizar las encuestas se formularon cuestionarios, las que fueron respondidas por los usuarios de la muestra. Se encuestaron a los usuarios de los departamentos de: Ciencia tecnología y salud, empresariales y administrativas, educación y humanidades, también a las oficinas de pedagogía, matemática y contabilidad.

Matriz de la recolección de la información:

Objetivos específicos	Fuentes	Técnicas utilizadas	Instrumento
Identificar las vulnerabilidades de la exposición de la información de los ordenadores a terceros.	Equipo de soporte técnico	Aplicación de entrevista Diagnostico técnico	Guía de entrevista Guía de observación Matriz de análisis de riesgo
	Usuarios de los equipos de cómputo	Aplicación de encuesta	Cuestionario en línea
	Computadoras	Diagnostico técnico	Guía de observación

Objetivos específicos	Fuentes	Técnicas utilizadas	Instrumento
			Capturas de pantalla
Seleccionar los procedimientos de seguridad de la información de la norma ISO 27001 aplicables en la FAREM-Estelí.	Estándar Internacional para la seguridad de la información.	Análisis de la información recopilada con relación a la vulnerabilidad actual de la información contenida en los equipos de cómputo.	Matriz de análisis de riesgo Análisis de riego Formulario de Google
Definir una propuesta de marco de referencia de seguridad de la información para el uso de los ordenadores, basadas en la norma ISO 27001.	Documento de propuesta de un marco de referencia definidas para la institución.	Redacción de un marco de referencia de seguridad de la información contenida en los equipos de cómputo.	Software de procesamiento de texto.
Conocer la percepción de los usuarios acerca de la utilidad de la aplicación de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.	Usuarios de los equipos de cómputo	Aplicación de encuesta	Cuestionario en línea

Tabla No.3: Matriz de recolección de la información.

8.9 Plan de análisis de la información

El análisis de la información consiste en categorizar y codificar los datos obtenidos del trabajo de campo, crear una matriz y elaborar representaciones gráficas, con el fin de elaborar conclusiones relevantes (Sampieri, Collado & Lucio, 2010).

Una vez aplicados los instrumentos de recolección de información se procedió a ponderar los factores de riesgo que nos permitieron identificar su impacto al materializarse el riesgo,

lográndose una valoración de estos: riesgos altos, medios, bajos e insignificantes para establecer medidas prioritarias, así como los recursos informáticos necesarios para su mitigación.

Para lograr lo anterior se utilizó una herramienta automatizada que devuelve la clasificación y posible impacto del riesgo de exposición de la información contenida en los ordenadores de la muestra.

También se usó una plataforma, se trata de la herramienta Formulario de Google, la cual permite crear encuestas y entrevistas en líneas y visualizar los datos recopilados en forma de gráficos.

De los instrumentos y procedimientos revisados y analizados, se desarrolló la propuesta del marco de referencia de seguridad de la información en el uso de los equipos de cómputo en la UNAN-Managua/FAREM-Estelí, basadas en la norma ISO 27001.

IX. Presupuesto

CONCEPTOS	PERSONAL	CANTIDAD	U.M	UNIT. $	TOTAL $
GASTOS DESARROLLO DE INVESTIGACION					
1. Transporte					
Pago de transporte	1	52	viajes	1.00	52.00
TOTAL TRANSPORTE					**52.00**
2. Alimentaciòn					
Viáticos	1	52	almuerzos	2.00	104.00
TOTAL ALIMENTACIÒN					**104.00**
3. Materiales					
Materiales de oficina Consumibles de oficina Cartucho, etc.)		1	Tóner	12.00	12.00
Papelería		1	Resma	3.00	3.00
Impresiones		7	Ejemplares	7.00	49.00
Encuadernación de documento		1	Ejemplares	25.00	25.00
TOTAL MATERIAL DIDÀCTICO					**89.00**
4. Medios y equipos					
Depreciación Equipos de Cómputo		1	Global		200.00
Elaboración de textos		7	Global		15.00
Internet		1	Global		120.00
TOTAL MEDIOS Y EQUIPOS					**335.00**
Imprevistos		1	Global	150.00	150.00
TOTAL DE IMPREVISTOS					**150.00**
GRAN TOTAL					**730.00**

Tabla No.4 Presupuesto.

X. Cronograma

No.	Actividades	Fechas de cumplimientos
1	Elaboración de instrumentos: entrevistas, encuetas, diagnóstico técnico.	29 febrero – 05 marzo 2016
2	Visitas a las oficinas de soporte técnico y usuarios finales de los ordenadores.	07 marzo – 19 marzo 2016
3	Análisis de la información recopilados.	21 marzo – 15 abril 2016
4	Definir Marco de referencia de seguridad de la información para el uso de los equipos de cómputos.	16 abril – 30 abril 2016
5	Propuesta de marco de referencia a la decanatura de FAREM-Estelí.	15 mayo 2016

Tabla No.5: Cronograma de actividades

XI. Resultados y Discusión

A continuación, se presentan y discuten los principales resultados de esta investigación, los cuales se organizan de acuerdo a los objetivos específicos (ver sistema de objetivos).

11.1 Vulnerabilidades de la exposición de la información de los ordenadores a terceros.

Según Carrasco (2013), los sistemas informáticos están sometidos a potenciales amenazas de seguridad de diversa índole, originadas tanto desde dentro de la propia organización, como desde fuera, procedentes de una amplia variedad de fuentes que ponen en peligro la disponibilidad, la integridad, la confidencialidad de la información.

Para la identificación de vulnerabilidades de la exposición de la información de los ordenadores a terceros, se procedió a ponderar los factores de riesgo que nos permitieron identificar su impacto al materializarse el riesgo, lográndose una valoración de estos. Para lo anterior se utilizó una herramienta automatizada que devuelve la clasificación y posible impacto del riesgo de exposición de la información contenida en los ordenadores de la muestra (ver anexo 14, 15 y 16: Matriz de análisis de riesgo). También se aplicaron entrevistas y encuesta a personal de soporte técnico y usuarios finales de los ordenadores, se realizó diagnóstico técnico in situ tomando como soporte de partida una guía de observación, lo que significó un gran aporte para lograr conocer si los actores antes mencionados tenían noción de la inseguridad a la que está expuesta la información contenida en los ordenadores que se les ha asignado en la institución.

Como resultado de la aplicación de los instrumentos de recolección de datos mencionados anteriormente, se identificaron tres grandes grupos de vulnerabilidades: Datos, Sistemas y Personal; los cuales a su vez contienen vulnerabilidades más específicas. Sin embargo, se discutirán algunas de cada grupo las que se consideran con mayor potencial de amenazas y que se pueden considerar como significativas en la exposición de la información:

a) Ausencia de copias de seguridad de los datos de la institución:

En los ordenadores se almacenan datos de la institución y datos personales, comprobándose por diagnóstico técnico in situ (ver anexos del 8 al 11), y por entrevista realizada a personal de soporte técnico que no existen normativas, planes, protocolos que permitan garantizar la seguridad de la información por medio de copias de respaldos existiendo entonces un alto grado de vulnerabilidad de la información lo que puede permitir la pérdida de la misma.

b) Mantenimiento de ordenadores:

La relación de la cantidad de ordenadores y personal técnico es muy desigual, y según entrevista a un miembro ésta área: "Esto nos lleva a realizar un mantenimiento al año por cada ordenador". De tal manera que se crea un espacio en tiempo muy considerable dejando las posibilidades de que la información no se considere confiable porque en ese lapso de tiempo puede ser manipulada, tergiversada, o en el peor de los casos alterada.

c) Programas de descargas de archivos de usuarios:

Se pudo constatar que en los ordenadores existen instalados programas de descargas de archivos de usuarios (ver anexos, 12 y 13), y se sabe que al realizar descargas se abre la posibilidad de infección del sistema de cómputo por virus informáticos, y otros tipos de códigos maliciosos que su principal intención es el daño de la información o la posición sin autorización de la misma.

d) Equipos de cómputos multiusuarios sin control de acceso:

Los equipos de cómputo son en su mayoría multiusuarios, por limitantes en la cantidad de ordenadores con relación a los funcionarios de la institución. Cuando se realizó diagnóstico técnico in situ, y corroborado por la entrevista realizada al personal de soporte técnico, se aprecia que no hay un control sobre la manera o forma de restringir que los usuarios solamente tengan acceso a su información y no

a la de los demás, creándose de esta manera riesgo que pueda ser tomada por cualquiera y utilizarla para propósitos de perjuicio o daño a la institución y a los mismos funcionarios de la FAREM-Estelí.

El personal de soporte técnico expresa claramente en la entrevista que no existe ningún documento oficial que sea el soporte para aplicar medidas de salvaguarda de uno de los activos más valiosos como es la información.

Como lo expresa un entrevistado del equipo de soporte técnico: "Los equipos son multiusuarios, por lo general tienen más de dos usuarios, particularmente en el caso de los docentes".

Tambien expresó: "Se dá este fenómeno porque la facultad no tiene la capacidad de brindar a cada trabajador o a cada docente el acceso a un equipo exclusivo".

Cuando fue abordado en el tema de que si existían medidas de salvaguarda de la información textualmente mencionó: "Una política o normativa por escrito avalada por las autoridades superiores que yo sepa no existe".

e) Ausencia de normativas de acceso a los equipos de cómputo:

Es importante que, en toda institución sin importar el tamaño existan políticas, marcos de referencia de seguridad de la información, controles, normativas, buenas prácticas. Al abordar a los usuarios finales de los ordenadores sobre este aspecto, entran en contradicción cuando en la aplicación de la encuesta se les abordaba sobre si era de su conocimiento la existencia de políticas de prohibición para acceso restringido a las áreas donde se encuentran las computadoras que usan para desempeñar sus labores en la institución y que la instalación de programas solamente la realice el personal autorizado. Hubo usuarios que afirmaron la existencia de prohibiciones, otros expresaron que no existen y también algunos dijeron que no sabían.

Como lo expresa un informante entrevistado del equipo de soporte técnico: "La instalación de programas la realiza cualquier usuario, aveces nos llaman, otras veces nos burlan y ellos hacen las instalaciones, las que luego nosotros encontramos en los equipos, instalan programas que no tienen nada que ver con sus funciones hasta a veces por hobby".

Continúa comentando cuando nuevamente se le pregunta por normativas de restricciones a los equipos de cómputos: "Como estamos actualmente y como ya había comentado anteriormente, no existe nada por escrito autorizado, que yo conozca no".

En escencia, personal de soporte técnico reafirma la carencia de normativas de acceso a equipos de computos. De hecho, ellos manifestaron que no existe una documentación oficial aplicable, tampoco una intención de que existe una. Por tanto, ellos consideran urgente mejorar la seguridad de la información contenida en los ordenadores, lo que a ellos permitirá brindar un servicio de calidad, desde las actividades técnicas.

f) Ausencia de una cuenta y contraseña de usuario:

Es muy alarmante encontrarse con equipos de cómputos multiusuarios que aparentemente tienen cuentas y contraseñas de usuarios pero que no son funcionales (ver anexos 4. 5. 6 y 7). Es decir, que basta con seleccionar cualquiera de las cuentas y ver por ejemplo qué cuentas de estudiantes tienen privilegios de administrador cuando no deberían de tenerlas, lo que les da la libertad de instalar aplicaciones sin autorización ni restricción alguna. Así mismo, se encontraron cuentas de administrador sin contraseñas y cuentas de usuarios con acceso libre o sea sin contraseña, lo que evidencia que no se está restringiendo el acceso a la

información almacenada en los ordenadores y que con facilidad puede ser tomada por cualquier persona.

Llama poderosamente la atención observar ordenadores con cuentas de usuarios y/o contraseñas, cuando el informante del equipo de soporte técnico manifestó: "En la institución no existen indicaciones o normativas, tampoco un marco de seguridad, que garanticen la aplicación de esta medida de protección, siendo el caso que fueron los mismos usuarios que por sentido común solicitaron formas de protección de su información".

Además, el entrevistado del equipo de soporte técnico agregó: "Por la misma razón de la no existencia de ningún reglamento aplicable a la protección de la información, las contraseñas no tienen ningún patrón de robustez, son creadas en conjunto con el usuario que lo solicita y entonces la contraseña es improvisada en ese mismo momento". A su vez comentó que "no hay ningún control sobre la administración de las cuentas de usuarios y contraseñas", es decir que exista una planificación y seguimiento de validez, caducidad, tiempo de concesión, mantenimiento y un patrón estándar a seguir en la construcción de la palabra secreta.

g) Cualquier usuario instala programas en los ordenadores:

Como se mencionó anteriormente, es evidente la amenaza causada por la posibilidad de instalación de programas por cualquier usuario. Cualquier persona puede acceder a internet desde las computadas, descargar programas o aplicaciones, las cuales pueden contener virus altamente perjudiciales. Así mismo, en las encuestas aplicadas a los participantes se les preguntó si descargaban archivos o programas para uso personal, por ejemplo, fotos, películas, música, etc. expresando que no se realizan. Sin embargo, las capturas de pantallas (Ver anexo 12 y 13) indican lo contrario. Esto es una evidencia clara de las amenazas de los servicios

de cómputos en la facultad y la ausencia de restricciones para evitar estas actividades por los usuarios finales.

11.2 Procedimientos de seguridad de la información de la norma ISO 27001 aplicables en la FAREM-Estelí

Basados en todos los dominios y controles de la ISO 27001, se procede a la selección de aquellos que se consideran apropiados y aplicables para el contexto particular de la institución, tomando aquellos que se ajustan al resultado de los riesgos encontrados y sustentados por las evidencias. La selección de dominios y controles son soportados por los resultados encontrados en la primera etapa de identificación de las vulnerabilidades de la exposición de la información de los ordenadores a terceros.

Cabe señalar que para la selección de los dominios y controles seleccionados fue realizada en consenso por representantes de todas las áreas sustantivas de la institución, los que posterior se conocerán con el denominador **"Comité de Seguridad de la Información".**

A continuación, se presenta el ISO/ IEC 27001:2013 con sus correspondientes dominios y controles.

Dominios y controles de la ISO/IEC 27001 que se tomaron para elaborar el marco de referencia

Núm.	Nombre	Descripción / Justificación
1	Objeto y campo de aplicación	Seleccionar los controles dentro del proceso de implementación del Sistema de Gestión de Seguridad de la Información - SGSI
2	Referencias normativas	La ISO/IEC 27000, es referenciada parcial o totalmente en el documento y es indispensable para su aplicación.
3	Términos y definiciones	Para los propósitos de este documento se aplican los términos y definiciones presentados en la norma ISO/IEC 27000.
4	Estructura de la norma	La norma ISO/IEC 27000, contiene 14 numérales de control de seguridad de la información que en su conjunto contienen más de 35 categorías de seguridad principales y 114 controles.
5	Políticas de seguridad de la información	

5.1	Directrices establecidas por la dirección para la seguridad de la información	Objetivo: Brindar orientación y apoyo por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes.
5.1.1	Políticas para la seguridad de la información	Control: Se debería definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y partes externas pertinentes.
5.1.2	Revisión de las políticas para seguridad de la información	Control: Las políticas para seguridad de la información se deberían revisar a intervalos planificados o si ocurren cambios significativos, para asegurar su conveniencia, adecuación y eficacia continuas.
6	Organización de la seguridad de la información	
6.1	Organización interna	Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y la operación de la seguridad de la información dentro de la organización.
6.1.1	Roles y responsabilidades para la seguridad de información	Control: Se deberían definir y asignar todas las responsabilidades de la seguridad de la información.
6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deberían separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
6.1.3	Contacto con las autoridades	Control: Se deberían mantener los contactos apropiados con las autoridades pertinentes.
7	Seguridad de los recursos humanos	
7.2	Durante la ejecución del empleo	Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.
7.2.1	Responsabilidades de la dirección	Control: La dirección debería exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
7.2.2	Toma de conciencia, educación y formación en la seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deberían recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos pertinentes para su cargo.
7.2.3	Proceso disciplinario	Control: Se debería contar con un proceso disciplinario formal el cual debería ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
8	Gestión de activos	
8.1	Responsabilidad por los activos	Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección apropiadas.

8.1.1	Inventario de activos	Control: Se deberían identificar los activos asociados con la información y las instalaciones de procesamiento de información, y se debería elaborar y mantener un inventario de estos activos.
8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deberían tener un propietario.
8.2	Clasificación de la información	Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.
9	Control de acceso	
9.1	Requisitos del negocio para control de acceso	Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.
9.1.1	Política de control de acceso	Control: Se debería establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de seguridad de la información.
9.2	Gestión de acceso de usuarios	Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.
9.2.1	Registro y cancelación del registro de usuarios	Control: Se debería implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
9.2.2	Suministro de acceso de usuarios	Control: Se debería implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso a todo tipo de usuarios para todos los sistemas y servicios.
9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debería restringir y controlar la asignación y uso de derechos de acceso privilegiado.
9.3	Responsabilidades de los usuarios	Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.
9.3.1	Uso de la información de autenticación secreta	Control: Se debería exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación secreta.
9.4	Control de acceso a sistemas y aplicaciones	Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.
9.4.1	Restricción de acceso Información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debería restringir de acuerdo con la política de control de acceso.
9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debería controlar mediante un proceso de ingreso seguro.
9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deberían ser interactivos y deberían asegurar la calidad de las contraseñas.
11	Seguridad física y del entorno	
11.2	Equipos	Objetivo: Prevenir la perdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.

11.2.1	Ubicación y protección de los equipos	Control: Los equipos deberían estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno, y las oportunidades para acceso no autorizado.
11.2.4	Mantenimiento de equipos	Control: Los equipos se deberían mantener correctamente para asegurar su disponibilidad e integridad continuas.
11.2.9	Política de escritorio limpio y pantalla limpia	Control: Se debería adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.
12	Seguridad de las operaciones	
12.2	Protección contra códigos maliciosos	Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.
12.2.1	Controles contra códigos maliciosos	Control: Se deberían implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.
12.3	Copias de respaldo	Objetivo: Proteger contra la perdida de datos.
12.3.1	Respaldo de información	Control: Se deberían hacer copias de respaldo de la información, del software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo aceptada.
12.4	Registro y seguimiento	Objetivo: Registrar eventos y generar evidencia.
12.4.1	Registro de eventos	Control: Se deberían elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.
12.4.2	Protección de la información de registro	Control: Las instalaciones y la información de registro se deberían proteger contra alteración y acceso no autorizado.
12.5	Control de software operacional	Objetivo: Asegurar la integridad de los sistemas operacionales.
12.5.1	Instalación de software en sistemas operativos	Control: Se deberían implementar procedimientos para controlar la instalación de software en sistemas operativos.
12.6	Gestión de la vulnerabilidad técnica	Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas.
12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debería obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.
12.6.2	Restricciones sobre la instalación de software	Control: Se deberían establecer e implementar las reglas para la instalación de software por parte de los usuarios.
12.7	Consideraciones sobre auditorias de sistemas de información	Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operacionales.

12.7.1	Información controles de auditoría de sistemas	Control: Los requisitos y actividades de auditoría que involucran la verificación de los sistemas operativos se deberían planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.
16	Gestión de incidentes de seguridad de la información	
16.1	Gestión de incidentes y mejoras en la seguridad de la información	Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.
16.1.1	Responsabilidad y procedimientos	Control: Se deberían establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
16.1.2	Reporte de eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deberían informar a través de los canales de gestión apropiados, tan pronto como sea posible.
16.1.3	Reporte de debilidades de seguridad de la información	Control: Se debería exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen e informen cualquier debilidad de seguridad de la información observada o sospechada en los sistemas o servicios.
16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	Control: Los eventos de seguridad de la información se deberían evaluar y se debería decidir si se van a clasificar como incidentes de seguridad de la información.
16.1.5	Respuesta a incidentes de seguridad de la información	Control: Se debería dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	Control: El conocimiento adquirido al analizar y resolver incidentes de seguridad de la información se debería usar para reducir la posibilidad o el impacto de incidentes futuros.
16.1.7	Recolección de evidencia	Control: La organización debería definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
17	Aspectos de seguridad de la información de la gestión de continuidad de negocio	

17.1	Continuidad de seguridad de la información	Objetivo: La continuidad de seguridad de la información se debería incluir en los sistemas de gestión de la continuidad de negocio de la organización.
17.1.1	Planificación de la continuidad de la seguridad de la información	Control: La organización debería determinar sus requisitos para la seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debería establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.
17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debería verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que son validos y eficaces durante situaciones adversas.
18	Cumplimiento	
18.2	Revisiones de seguridad de la información	Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.
18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación (es decir, los objetivos de control, los controles, las políticas, los procesos y los procedimientos para seguridad de la información) se deberían revisar independientemente a intervalos planificados o cuando ocurran cambios significativos.

Tabla No.6: Dominios y controles de la ISO/IEC 27001 que se tomaron para elaborar el marco de referencia

11.3 Definición de una propuesta de marco de referencia de seguridad de la información para el uso de los ordenadores, basadas en la norma ISO 27001

Lo anterior da paso a la Declaración de Aplicabilidad (SoA por las siglas en inglés de Statement of Applicability), que en otras palabras es un documento, conteniendo la propuesta de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.

Fueron tomados en cuenta los dominios y controles evaluados y seleccionados por el Comité de Seguridad de la Información. (Ver a continuación documento "Marco de referencia de seguridad de

la información en el uso de los equipos de cómputo en la UNAN-Managua/ FAREM-Estelí, aplicando la norma ISO 27001").

11.3.1 Marco de referencia de seguridad de la información en el uso de los equipos de cómputo en la UNAN-Managua / FAREM-Estelí, aplicando la norma ISO 27001

Introducción

La información es un activo esencial y es decisiva para la viabilidad de una organización. Adopta diferentes formas, impresa, escrita en papel, digital, transmitida por correo, mostrada en videos o hablada en conversaciones.

Debido a que está disponible en ambientes cada vez más interconectados, está expuesta a amenazas y vulnerabilidades.

La seguridad de la información es la protección de la información contra una amplia gama de amenazas; para minimizar los daños, ampliar las oportunidades de las instituciones, maximizar el retorno de las inversiones y asegurar la continuidad del negocio.

Se va logrando mediante la implementación de un conjunto adecuado de políticas, marcos de referencias, procesos, procedimientos, organización, controles, hardware y software y, lo más importante, mediante comportamientos éticos de las personas.

Términos y definiciones

Con el objeto de precisar el alcance de los principales conceptos utilizados en este documento, se transcriben las definiciones que sobre los mismos se han incluido en el en este marco de referencia de Seguridad de la Información.

Seguridad de la Información: La seguridad de la información se entiende como la preservación de las siguientes características:

- **Confidencialidad**: Se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a la misma.

- **Integridad**: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.
- **Disponibilidad**: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.

Adicionalmente, deberán considerarse los conceptos de:

- **Autenticidad**: busca asegurar la validez de la información en tiempo, forma y distribución. Asimismo, se garantiza el origen de la información, validando el emisor para evitar suplantación de identidades.
- **Auditabilidad**: define que todos los eventos de un sistema deben poder ser registrados para su control posterior.
- **Confiabilidad de la Información**: es decir, que la información generada sea adecuada para sustentar la toma de decisiones y la ejecución de las misiones y funciones.

Información: Se refiere a toda comunicación o representación de conocimiento como datos, en cualquier forma, con inclusión de formas textuales, numéricas, gráficas, cartográficas, narrativas o audiovisuales, y en cualquier medio, ya sea magnético, en papel, en pantallas de computadoras, audiovisual u otro.

Sistema de Información: Se refiere a un conjunto independiente de recursos de información organizados para la recopilación, procesamiento, mantenimiento, transmisión y difusión de información según determinados procedimientos, tanto automatizados como manuales.

Tecnología de la Información: Se refiere al hardware y software operados por los colaboradores de la institución o por un tercero que procese información en su nombre, para llevar a cabo una función propia de la entidad, sin tener en cuenta la tecnología utilizada, ya se trate de computación de datos, telecomunicaciones u otro tipo.

Comité de Seguridad de la Información: El Comité de Seguridad de la Información, es un cuerpo integrado por representantes de todas las áreas sustantivas del Organismo, destinado a garantizar el apoyo manifiesto de las autoridades a las iniciativas de seguridad.

Responsable de Seguridad Informática: Es la persona que cumple la función de supervisar el cumplimiento del presente marco de referencia y de asesorar en materia de seguridad de la información a los integrantes de la institución que así lo requieran.

Marco de referencia de la seguridad de la información.

Propósito

Proteger los recursos de información de la institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad y confiabilidad de la información.

Definición del alcance:

Este documento de marco de referencia aplica a los departamentos: Ciencia, Tecnología y Salud, Ciencias Empresariales y Administrativas y Educación y Humanidades, así también a oficinas de pedagogía, matemática y contabilidad de la UNAN, Managua / FAREM, Estelí.

Selección de controles y SOA

Basados en los dominios y controles de la ISO/IEC 27001, se procede a la selección de los apropiados y aplicables para el contexto particular de la institución, tomando aquellos que se ajustan al resultado de los riesgos encontrados y sustentados por las evidencias.

Lo anterior da paso a la Declaración de Aplicabilidad (SoA por las siglas en inglés de Statement of Applicability), que en otras palabras es un documento, conteniendo la propuesta de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.

Partiendo inicialmente con la formación del ente rector de la seguridad de la información en los ordenadores de la institución "Comité de Seguridad de la Información."

Infraestructura de la Seguridad de la Información

Comité de Seguridad de la Información:

Está conformado por los integrantes de todas las áreas sustantivas de la institución, en este sentido nos referimos particularmente, al decanato, administración, directores de departamentos (Ciencia, Tecnología y Salud, Ciencias Empresariales y Administrativas y Educación y humanidades) y responsable del área de contabilidad, destinadas a garantizar el apoyo a las iniciativas de seguridad.

En términos generales las iniciativas tienen como principales intenciones:

a) Proteger los recursos de información de la institución y la tecnología utilizada para su procesamiento, frente a amenazas, internas o externas, deliberadas o accidentales, con el fin de asegurar el cumplimiento de la confidencialidad, integridad, disponibilidad de la información.

b) Considerar la propuesta de (asegurar la implementación) las medidas de seguridad comprendidas en el marco de referencia, identificando los recursos necesarios, sin que ello implique necesariamente la asignación de otros adicionales.

c) Promover la difusión y apoyo a la seguridad de la información dentro de la institución.

d) Mantener el marco de referencia de seguridad de información de la institución actualizado, a efectos de asegurar su vigencia y nivel de eficacia.

Asignación de responsabilidades en materia de seguridad de la información

El decanato es la máxima autoridad y por ende el facultado para asignar las funciones relativas a la seguridad informática de la institución, quien puede delegar responsabilidades puntuales según funciones de puestos de trabajo que están vinculados directamente con los sistemas informáticos elementales (entiéndase a los ordenadores distribuidos en las diferentes áreas de la institución) a quienes en adelante le llamaremos el o los "Responsable de Seguridad Informática", quien tendrá a cargo las funciones relativas a la seguridad de los sistemas de información, lo cual incluye la supervisión de todos los aspectos inherentes a seguridad informática tratados en la presente marco de referencia.

El Comité de Seguridad de la Información propondrá a la autoridad superior que corresponda para su aprobación, la definición y asignación de las responsabilidades por áreas que se detallan a continuación.

Área	Rol	Nombre	Responsabilidades
Departamentos: 1.Ciencias, Tecnología y Salud. 2.Ciencias empresariales y Administrativas. 3.Educación y Humanidades	Soporte técnico: - Hardware. - Software.	Persona responsable de Soporte Técnico.	- Mantenimiento preventivo y correctivo de partes de los ordenadores. - Revisión de funcionamiento de UPS y sus acumuladores. - Creación y configuración de cuentas de usuarios. - Instalación y desinstalación de software en los ordenadores. - Velar por que las definiciones de actualizaciones de los anti virus sean las más recientes.
Oficinas de: 1.Matemática 2.Pedagogía			
Contabilidad			

Tabla No.7: Definición y asignación de las responsabilidades por áreas.

Recomendaciones:

Estas son algunas recomendaciones del marco de referencia que le ayudarán a aprovechar al máximo el uso de los servicios informáticos de la institución.

a) Ser respetuosos de los compañeros de trabajo y de su trabajo.

b) Evitar dañar el ordenador asignado.

c) No compartir su propia contraseña de acceso con ninguna persona.

d) No gastar recursos limitados tales como espacios de almacenamiento en los discos duros de los ordenadores.

e) No acceder a los archivos ni al trabajo de otras personas.

f) Si se encuentra por accidente algún material ilegal u ofensivo, avisar inmediatamente al comité de seguridad de la información.

g) Asumir la responsabilidad por sus propias acciones y por las sanciones que se apliquen al haber alguna infracción en los controles que forman el marco de referencia de seguridad de la información.

Adecuación de controles del ISO 27001 y creación de SOA

Dominio: A.5: Políticas de seguridad de la información.

Control: A.5.1: Directrices establecidas por la dirección para la seguridad de la información.

a) Las directrices del marco de referencia para la seguridad de la información están relacionadas con los ordenadores que les son asignados a los usuarios, aspectos relacionados con la protección de la información creada y manipuladas almacenada en los discos duros. Es de estricto cumplimiento todas las disposiciones reflejadas en el presente documento.

b) Los controles del marco de referencia de seguridad informática establecidos dentro de este documento son la base para la protección de los activos tecnológicos e información de la institución.

Control: A.5.1.1: Políticas para la seguridad de la información.

a) Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la institución, así como el estricto apego al marco de referencia de seguridad informática para usuarios.

b) Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir los controles de seguridad informática para usuarios del presente marco de referencia.

Control: A.5.1.2: Revisión de las políticas para la seguridad de la información.

a) Dentro del desarrollo del ciclo de revisiones y mejoras continuas de los controles del marco de referencia se establece que las personas asignadas en el apartado de responsabilidades en materia de seguridad de la información, y que fueron aprobadas con el consentimiento del Comité de Seguridad de la Información realizarán dicha actividad de revisión cada cuatro meses a partir de la fecha de puesta en marcha del marco de referencia.

b) El marco de referencia de seguridad de la información debe ser revisado para asegurar que se cumplan los objetivos marcados por la organización.

En concreto se deben revisar los siguientes documentos:

- El informe de las auditorías internas que recoge el estado de los controles y de las incidencias detectadas.
- Los informes que el responsable de seguridad informática dirige al Comité de Seguridad de la Información. Estos documentos son una fuente muy valiosa para el seguimiento, ya que reflejan el estado del marco de referencia y los puntos que requieren la supervisión más específica.
- Informe sobre las acciones realizadas por parte de los diferentes actores involucrados en el sistema.
- Informe sobre el estado de las incidencias reportadas y la solución a las mismas.
- Informe sobre los cambios sufridos en la estructura de la institución.

Dominio: A.6: Organización de la Seguridad de la Información.

Control: A.6.1: Organización Interna.

a) La institución debe establecer una estructura que sea su responsabilidad la seguridad de la información. De forma elemental debe conformase de la siguiente manera y jerárquicamente como sigue.

1. Comité de Seguridad de la Información.

2. Responsable de Seguridad Informática.
3. Usuarios finales de bienes y servicios informáticos.

Control: A.6.1.1: Roles y responsabilidades para la seguridad de la información.

a) Una vez conformado el Comité de Seguridad de la Información, es responsabilidad directa de éste la determinación y asignación de las responsabilidades de seguridad informática a las personas cuyos roles son afines a las actividades de soporte técnico de hardware y software.

b) El responsable de seguridad informática tiene a cargo el seguimiento, documentación y análisis de los incidentes de seguridad reportados, así como su comunicación al Comité de Seguridad de la Información, a los propietarios de la información.

c) El Comité de Seguridad de la Información será responsable de implementar los medios y canales necesarios para que el responsable de seguridad informática maneje los reportes de incidentes y anomalías. Asimismo, dicho Comité, tomará conocimiento, efectuará el seguimiento de la investigación, controlará la evolución e impulsará la resolución de los incidentes relativos a la seguridad.

d) Los usuarios finales de bienes y servicios informáticos son responsables del reporte de debilidades e incidentes de seguridad que oportunamente se detecten como usuarios.

Control: A.6.1.3: Contactos con las autoridades.

a) Se establece únicamente como medios de comunicación con aspectos relacionados con la seguridad informática los siguientes:

1. Correo electrónico institucional.
2. Extensiones telefónicas dentro de la institución.

Comunicación de Incidentes Relativos a la Seguridad.

a) Los incidentes relativos a la seguridad serán comunicados a través de canales establecidos tan pronto como sea posible. Se establecerá un procedimiento formal de comunicación y de respuesta a incidentes, indicando la acción que ha de emprenderse al recibir un informe sobre incidentes. Dicho procedimiento deberá contemplar que, ante la detección de un supuesto incidente o violación de la seguridad, el responsable de seguridad informática sea informado tan pronto como se haya tomado conocimiento. Este indicará los recursos necesarios para la investigación y resolución del incidente, y se encargará de su monitoreo. Asimismo, mantendrá al Comité de Seguridad al tanto de la ocurrencia de incidentes de seguridad.

Comunicación de Debilidades en Materia de Seguridad.

a) Los usuarios finales de bienes y servicios informáticos, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al responsable de seguridad informática.

Comunicación de Anomalías del Software.

a) Se establecerán procedimientos para la comunicación de anomalías de software, los cuales deberán contemplar:

- Registrar los síntomas del problema y los mensajes que aparecen en pantalla.
- Establecer las medidas de aplicación inmediata ante la presencia de una anomalía.
- Alertar inmediatamente al responsable de seguridad informática o del activo de que se trate.
- La recuperación será realizada por personal experimentado, adecuadamente habilitado y autorizado.

Dominio: A.7: Seguridad de los recursos humanos.

Control: A.7.2: Durante la ejecución del empleo.

a) El responsable de la administración de recursos humanos de la institución creará e implementará mecanismos para que los usuarios finales de bienes y servicios informáticos, tomen conciencia de sus responsabilidades de seguridad de la información y la cumplan.

Control: A.7.2.1: Responsabilidad de la dirección.

a) El responsable de la administración de recursos humanos de la institución incluirá las funciones relativas a la seguridad de la información en las descripciones de puestos de los empleados, informará a todo el personal de sus obligaciones respecto del cumplimiento del marco de referencia de Seguridad de la Información.

Control: A.7.2.2: Toma de conciencia, educación y formación en la seguridad de la información.

a) El responsable de la administración de recurso humanos de la institución, garantizará que todos los colaboradores, cuando sea pertinente, reciban una adecuada capacitación y actualización periódica en materia del marco de referencia, controles y procedimientos de la institución. Esto comprende los requerimientos de seguridad y las responsabilidades asumidas por los mismo, así como la capacitación referida al uso correcto de las instalaciones de procesamiento de información y el uso correcto de los recursos en general, como por ejemplo su estación de trabajo.

Control: A.7.2.3: Proceso disciplinario.

a) El incumplimiento de las disposiciones establecidas en el marco de referencia de seguridad de la información tendrá como resultado la aplicación de diversas sanciones, conforme a la magnitud y característica del aspecto no cumplido.

b) Al detectarse un incumplimiento de los controles en el marco de referencia, se aplicarán los siguientes criterios y sanciones:

1. La primera vez que el usuario haya incumplido uno de los controles el Comité de Seguridad de la Información notificará por escrito al responsable de la falta y le recordará revisar el marco de referencia.
2. De presentarse un segundo incumplimiento en los controles, el Comité de Seguridad de la Información notificará por escrito al jefe inmediato del responsable de la falta, informándole el tipo y contenido de la falta.
3. En caso de presentarse un tercer incumplimiento en los controles, por parte del mismo usuario, causará la anexión a su expediente laboral de un memorándum y el Comité de Seguridad de la Información determinará si es necesario aplicar sanciones administrativas adicionales.

Dominio: A.8: Gestión de activos.

Control: A.8.1: Responsabilidad por los activos.

a) Las autoridades correspondientes entiéndase, el responsable de la administración de recursos humanos de la institución atreves de su delegado (encargado de inventarios), directores de departamentos asignarán y entregarán los equipos de cómputo a los usuarios finales de bienes y servicios informáticos, adjunto a lo anterior un documento conteniendo un listado detallado de la de las características técnicas del ordenador el que será firmado como evidencia de la concesión, del cuido, protección del activo y la implementación de los controles de seguridad de la información que en ellos se manipularán.

Control: A.8.1.1: Inventario de activos.

a) Se identificarán los activos importantes asociados a cada sistema de información, sus respectivos propietarios y su ubicación, para luego elaborar un inventario con dicha información.

b) El encargado de elaborar el inventario y mantenerlo actualizado es el personal asignado por la administración de recursos humanos de la institución para esta actividad.

Control: A.8.2: Propiedad de los activos.

a) El responsable de seguridad informática en conjunto con el administrador de recursos humanos de la institución o en su defecto a quien éste designe, son los encargados de crear, actualizar y verificar periódicamente un inventario con los nombres, apellidos y detalles de activos de los usuarios finales de los ordenadores.

Control: A.8.2: Clasificación de la información.

a) El usuario final de cada ordenador es el responsable de clasificar la información en ellos contenidos. Para clasificar un activo de información, se evaluarán las tres características de la información en las cuales se basa la seguridad confidencialidad, integridad, disponibilidad.

Dominio: A.9: Control de acceso.

Control: A.9.1: Requisitos del negocio para control de acceso.

a) Los mecanismos de control y acceso físico para el personal y terceros deben permitir el acceso a las instalaciones y áreas restringidas de la institución, sólo a personas autorizadas para la salvaguarda de los equipos de cómputo y la información en ellos contenida.

b) No permitir y no facilitar el uso de los sistemas informáticos de la institución a personas no autorizadas.

Control: A.9.1.1: Políticas de control de acceso.

a) Los controles de acceso, serán determinados por el Comité de Seguridad de la Información y el responsable de seguridad informática, a fin de permitir el acceso sólo al personal *autorizado.*

b) El responsable de seguridad informática definirá un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario.

Control: A.9.2: Gestión de acceso a usuarios.

a) Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado; esto es, de su identificador de usuario y contraseña necesarios para acceder a la información y a los equipos de cómputos de la institución, por lo cual deberá mantenerlo de forma confidencial.

b) El acceso a los equipos de cómputo para personal externo debe ser autorizado por el usuario a quien fue asignado el ordenador, asumiendo de manera inmediata toda la responsabilidad que esa acción conlleve, además deberá notificarlo por escrito al responsable de seguridad informática de la institución.

Control: A.9.2.1: Suministro de acceso de usuarios.

a) El responsable de seguridad informática, es el único autorizado en crear mecanismos de acceso de usuarios a los equipos de cómputos pertenecientes al inventario de activos de la institución.

b) Cuando un usuario recibe una cuenta, debe firmar un documento donde declara conocer las políticas, marcos de referencia y procedimientos de seguridad, y acepta sus responsabilidades con relación al uso de esa cuenta.

Control: A.9.2.1: Gestión de derechos de acceso privilegiado.

a) Se limitará y controlará la asignación y uso de privilegios, debido a que el uso inadecuado de los privilegios de acceso resulta frecuentemente en el factor más importante que contribuye a la falla de los sistemas a los que se ha accedido ilegalmente. Los sistemas multiusuario que requieren protección contra accesos no autorizados, deben prever una asignación de privilegios controlada mediante un proceso de autorización formal.

b) El responsable de seguridad informática, controla y determina el nivel de privilegios y/o restricciones se le asigna a cada uno de los usuarios finales de bienes y servicios informáticos, basado en los roles de actividades que estos realizan dentro de la institución.

Dominio: A.9.3: Responsabilidades de los usuarios.

a) Todo usuario de bienes y servicios informáticos se comprometen a conducirse bajo los principios de confidencialidad de la información y de uso adecuado de los recursos informáticos de la institución, así como el estricto apego al Marco de referencia de Seguridad Informática para usuarios.

b) Es responsabilidad de los usuarios de bienes y servicios informáticos cumplir controles de seguridad informática para usuarios del presente marco de referencia.

c) Los usuarios deben rendir cuentas y responsabilizarse por la salvaguarda de los activos de la institución, esto es los equipos de cómputo bajo su responsabilidad, la información contenida en los medios de almacenamiento de los ordenadores. Son los responsables de proteger los programas y datos contra pérdida o daño.

Control: A.9.3.1: Uso de la información de la autenticación.

a) Todos los usuarios deberán autenticarse por los mecanismos de control de acceso provistos por la el responsable de seguridad informática, para de poder usar los equipos de cómputos.

b) Los usuarios no deben proporcionar información a personal externo, de los mecanismos de control de acceso a las instalaciones y equipos de cómputos de la institución.

Control: A.9.4: Control de acceso a sistemas y aplicaciones.

a) Cada usuario debe hacer una solicitud de una cuenta o el cambio de privilegios, debe ser hecha por escrito y debe ser debidamente aprobada por el responsable de seguridad informática.

b) Cualquier cambio en los roles y responsabilidades de los usuarios que modifique sus privilegios de acceso, deberán ser notificados por escrito o vía correo electrónico a al responsable de seguridad informática, con el visto bueno del titular del área solicitante, para realizar el ajuste.

Control: A.9.4.1: Restricción de acceso de información.

a) Los usuarios tienen prohibido compartir su identificador de usuario y contraseña, ya que todo lo que ocurra con ese identificador y contraseña será responsabilidad exclusiva del usuario al que pertenezcan, salvo prueba de que le fueron usurpados esos controles.

b) Los usuarios tienen prohibido usar el identificador de usuario y contraseña de otros, aunque ellos les insistan en usarlo.

Control: A.9.4.2: Procedimiento de ingreso seguro.

a) Los usuarios solamente deben acceder al equipo de cómputo en la cuenta que se le ha asignado, usando el procedimiento de autenticación y autorización creado para cada uno de ellos.

b) Los usuarios deberán mantener sus equipos de cómputo con controles de acceso además de sus contraseñas, protectores de pantalla previamente instalados y autorizados, como una medida de seguridad cuando el usuario necesita ausentarse de su escritorio por un tiempo.

c) Cuando el usuario ingrese su contraseña debe verificar que terceras personas no observen los que está digitando desde el teclado.

Control: A.9.4.3: Sistema de gestión de contraseñas.

a) La asignación de la contraseña para acceso a los equipos de cómputos, debe ser realizada de forma individual, por lo que queda prohibido el uso de contraseñas compartidas.

b) Cuando un usuario olvide, bloquee o extravíe su contraseña, deberá reportarlo por escrito al responsable de seguridad informática, para que se le proporcione una nueva contraseña.

c) La obtención o cambio de una contraseña debe hacerse de forma segura; el usuario deberá acreditarse como colaborador de la institución.

d) Está prohibido que los identificadores de usuarios y contraseñas se encuentren de forma visible en cualquier medio impreso o escrito en el área de trabajo del usuario, de manera de que se permita a personas no autorizadas su conocimiento.

Lineamientos para la construcción de sus contraseñas:

- No deben contener números consecutivos.
- Deben estar compuestos de al menos seis (6) caracteres y máximo diez (10). Estos caracteres deben ser alfanuméricos, o sea, números y letras;
- Deben ser difíciles de adivinar, esto implica que las contraseñas no deben relacionarse con el trabajo o la vida personal del usuario.
- Deben ser diferentes a las contraseñas que se hayan usado previamente.

e) La contraseña podrá ser cambiada por requerimiento del dueño de la cuenta.

f) Todo usuario que tenga la sospecha de que su contraseña es conocida por otra persona, tendrá la obligación de cambiarlo inmediatamente.

g) Los usuarios no deben almacenar las contraseñas en ningún programa o sistema que proporcione esta facilidad.

h) No debe concederse una cuenta a personas que no sean colaboradores de la institución a menos que estén debidamente autorizados por el Responsable de Seguridad Informática, en cuyo caso la cuenta debe expirar automáticamente al cabo de un lapso de 30 días.

i) Toda cuenta y contraseña queda automáticamente suspendida después de un cierto periodo de inactividad. El periodo recomendado es de 30 días.

Dominio: A.11: Seguridad física y del entorno.

Control: A.11.2: *Equipos.*

a) El responsable de seguridad informática debe de diseñar y aplicar procedimientos para el trabajo en áreas seguras.

b) Los equipos de la institución sólo deben usarse para actividades de trabajo y no para otros fines, tales como juegos y pasatiempos.

c) Deben protegerse los equipos para disminuir el riesgo de robo, destrucción, y mal uso. Las medidas que se recomiendan incluyen el uso de vigilantes y cerradura con llave.

d) Los equipos deben marcarse para su identificación y control de inventario. Los registros de inventario deben mantenerse actualizados.

Control: A.11.2.1: Ubicación y protección de los equipos.

a) Los equipos de cómputos de la institución sólo deben usarse en un ambiente seguro. Se considera que un ambiente es seguro cuando se han implantado las medidas de control apropiadas para proteger el software, el hardware y los datos. Esas medidas deben estar acorde a la importancia de los datos y la naturaleza de riesgos previsibles.

b) No se permite fumar, comer o beber mientras se está usando un ordenador.

c) Deben protegerse los ordenadores de riesgos del medioambiente (por ejemplo, polvo, incendio y agua).

d) Deben usarse protectores contra fluctuaciones de energía eléctrica deben usarse fuentes de poder interrumpibles (UPS).

e) Cualquier falla en los ordenadores debe reportarse inmediatamente ya que podría causar problemas serios como pérdida de la información o indisponibilidad de los servicios.

f) No pueden moverse los ordenadores o reubicarlos sin permiso. Para llevar un ordenador fuera de la institución se requiere una autorización escrita.

g) Queda prohibido que el usuario abra o desarme los ordenadores, únicamente el personal asignado para tal responsabilidad.

h) El ordenador o cualquier recurso de tecnología de equipo información que sufra alguna avería por maltrato, descuido o negligencia por parte del usuario, deberá cubrir el valor de

la reparación o reposición del equipo o accesorio afectado. Para tal caso se determinará la causa de dicho desperfecto.

i) La pérdida o robo de cualquier componente de hardware o programa de software debe ser reportada inmediatamente.

j) Si un ordenador tiene acceso a datos confidenciales, debe poseer un mecanismo de control de acceso especial, preferiblemente por hardware.

k) Los datos confidenciales que aparezcan en la pantalla deben protegerse de ser vistos por otras personas mediante disposición apropiada del mobiliario de la oficina y protector de pantalla. Cuando ya no se necesiten o no sean de utilidad, los datos confidenciales se deben borrar.

l) No debe utilizarse software bajado de Internet y en general software que provenga de una fuente no confiable, a menos que haya sido comprobado en forma rigurosa y que esté aprobado su uso por el responsable de seguridad informática.

m) Se prohíbe estrictamente la instalación de software no autorizado, incluyendo el que haya sido adquirido por el propio usuario. Así mismo, no se permite el uso de software de distribución gratuita o shareware, a menos que haya sido previamente aprobado por el responsable de seguridad informática.

Control: A.11.2.4: Manteamiento de equipos.

a) Los mantenimientos de hardware y software en los ordenadores, únicamente están autorizados a realizarlos el personal de soporte técnico de la institución. Los cuales deben enviar por escrito al responsable de seguridad informática un cronograma de la realización de los mismos.

- Instalación y /o desinstalación de programas
- Reparación y /o cambios de piezas en los ordenadores.
- Reparación y /o cambio de UPS (sistemas de respaldos de energía)

b) Los usuarios deben de respetar y no modificar la configuración de hardware y software establecida por el personal de soporte técnico de Informática.

Control: A.11.2.9: Política de escritorio limpio y pantalla limpia.

a) Es responsabilidad de los colaboradores de la institución mantener un escritorio limpio para proteger documentos en papel y dispositivos de almacenamiento removibles, esto es guardar bajo llave en el escritorio documentos y dispositivos móviles que contengan información sensible.

b) Es una obligación de los usuarios de los ordenadores garantizar pantallas limpias (escritorio del ordenador), a fin de reducir los riesgos de acceso no autorizado, pérdida y daño de la información, tanto durante el horario normal de trabajo como fuera del mismo. Por tanto, si deja por alguna razón su ordenador en horas laborales hábiles y se traslada hacia otro punto de la institución, debe activar el bloqueo de pantalla el que deberá mostrar la solicitud de autenticación y autorización.

Dominio: A.12: Seguridad de las operaciones.

Control: A.12.2: Protección contra códigos maliciosos.

a) Debe instalarse y activarse una herramienta antivirus, la cual debe mantenerse actualizada. Si se detecta la presencia de un virus u otro agente potencialmente peligroso, se debe notificar inmediatamente al responsable de seguridad informática y poner el ordenador en cuarentena hasta que el problema sea resuelto.

b) Ningún usuario debe intencionalmente escribir, generar, compilar, copiar, propagar, ejecutar o tratar de introducir código de computadora diseñado para autoreplicarse, dañar o en otros casos impedir el funcionamiento de cualquier ordenador, archivos de sistema o software. Tampoco debe probarlos en cualquiera de los ordenadores de la institución.

c) Debe revisarse todo dispositivo externo de almacenamiento de información que se conecte al ordenador antes de manipular la información en él contenida.

d) No deben usarse documentos en digital si no se conoce su procedencia, de ser necesario debe antes revisarse con una herramienta anti virus.

e) Cualquier usuario que sospeche de alguna infección por virus informático, deberá dejar de usar inmediatamente el equipo y llamar al equipo de soporte técnico para la detección y erradicación del virus.

Control: A.12.3: Copias de respaldo.

a) En caso de uso cotidiano y de desperfecto en el funcionamiento de los ordenadores, es responsabilidad de los usuarios asegurarse de respaldar la información que considere relevante.

b) Al enviar el ordenador a reparación, borrar aquella información sensible que se encuentre en el equipo previendo así la pérdida involuntaria de información, derivada de proceso de reparación, solicitando la asesoría del personal de soporte técnico.

c) Las copias de respaldo deben guardarse en un lugar seguro, a prueba de hurto, incendio e inundaciones. Los programas y datos vitales para la operación de institución deben guardarse en otra sede, lejos del edificio.

Control: A.12.4: Registro y Seguimiento.

Control: A.12.4.1: Registro a eventos.

a) Se establecen funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad. Esto implica que el responsable de seguridad informática, los miembros del equipo de soporte técnico deben crear una herramienta para registrar todos los eventos suscitados relativos a las funciones asignadas con relación a la seguridad de la información contenidas en los ordenadores. Dicha herramienta debe permitir la creación de una base de conocimiento que pueda ser consultas para la toma de decisiones.

Control: A.12.4.2: Protección de la información de registro.

a) Las bitácoras generadas por la herramienta de registro de eventos deben guardarse en un lugar seguro, donde solamente puedan acceder el responsable de seguridad informática y el personal que conforma el equipo de soporte técnico de la institución. Siendo responsabilidad de ambas figuras la garantía de la protección de éstas.

Control: A.12.5: Control de Software operacional.

a) Es obligación del responsable de seguridad informática y del equipo de soporte técnico garantizar la uniformidad de software en los ordenadores de la institución.

Control: A.12.5.1: Instalación de software en sistemas operativos.

a) El equipo de soporte técnico debe crear un listado de los programas que se instalarán en los ordenadores de la institución, para la aprobación por parte del responsable de seguridad informática. Únicamente solo y solamente estos programas son los que se instalaran uniformemente en los ordenadores.

Control: A.12.6: Gestión de la vulnerabilidad técnica.

Control: A.12.6.1: Gestión de las vulnerabilidades técnicas.

a) El responsable de seguridad informática en conjunto con el equipo de soporte técnico deben registrar los motivos, así como las evidencias de las vulnerabilidades de índole técnico por cada miembro del equipo, relativos a seguridad de la información. Esto implica que el responsable de seguridad informática, los miembros del equipo de soporte técnico deben crear una herramienta para registrar todos los eventos suscitados.

Control: A.12.6.2: Restricciones sobre la instalación de software.

a) Los usuarios que requieran la instalación de software, deberán justificar su uso y solicitar su autorización al responsable de seguridad informática, por escrito y firmado por jefe inmediato superior, indicando el equipo de cómputo donde se instalará el software y el período que permanecerá dicha instalación. El equipo de soporte técnico procederá a realizar la instalación solicitada.

Control: A.12.7: Consideraciones sobre auditorias de sistemas de información:

a) El responsable de seguridad informática, debe planificar en tiempo y forma, delegar personal para la realización de auditorías informáticas internar, para dar seguimiento al cumplimiento del marco de referencia de seguridad de la información.

Control: A.12.7.1: Informacion controles de auditoria de sistemas.

a) La información, evidencias, pruebas de inconsistencias encontradas en las auditorias informáticas serán usada por el responsable de seguridad informática, para minimizar las interrupciones en los procesos de la institución.

Dominio: A.16: Gestión de incidentes de seguridad de la información.

Control: A.16.1: Gestión de incidentes y mejoras de seguridad de la información.

a) El responsable de seguridad informática debe de gestionar efectivamente con un enfoque coherente y eficaz los resultados de las auditorias informáticas internas, el registro de las vulnerabilidades técnicas para ser tomadas en cuenta para las mejoras del marco de referencia de seguridad de la información de la institución.

Control: A.16.1.1: Responsabilidad y procedimientos.

a) El Comité de Seguridad e la Información y el responsable de seguridad informática, establecerán responsabilidades, funciones y procedimientos de manejo de incidentes garantizando una respuesta rápida, eficaz y sistemática a los incidentes relativos a seguridad.

Control: A.16.1.2: Reporte de eventos de seguridad de la información.

a) Es obligatorio para el responsable de seguridad informática y el equipo de soporte técnico diariamente reportar por medio de las formas oficiales y herramientas de registro de incidentes creada para la institución absolutamente todos los eventos presentados durante el transcurso del día.

Control: A.16.1.3: Reporte de debilidades de seguridad de la información.

a) Se debe reportar al finalizar el día atreves de los canales de comunicación y herramientas oficialmente establecidos los resultados de la aplicación de procedimientos de manejo de incidentes.

Control: A.16.1.4: Evaluación de eventos de seguridad de la información y decisiones sobre ellos.

a) El Comité de Seguridad e la Información y el responsable de seguridad informática, deben crear cronograma para programar reuniones y / o reunirse extraordinarias para evaluación de eventos de seguridad acontecidos, y decidir si se toman como incidentes de seguridad de la información.

Control: A.16.1.5: Respuestas a incidentes de seguridad de la información.

a) El Comité de Seguridad e la Información y el responsable de seguridad informática, deben tomar decisiones para dar respuesta a los incidentes de seguridad de la información de acuerdo con los procedimientos de manejo de incidentes documentados.

Control: A.16.1.6: Aprendizajes obtenidos de los incidentes de seguridad de la información.

a) Basados en la herramienta de registro y seguimiento de: eventos, gestión de vulnerabilidades técnicas, gestión de incidentes se deben crear planes de actualización y /o capacitación a personal involucrado en las funciones de seguridad de la información de la institución.

Control: A.16.1.7: Recolección de evidencias.

a) Es responsabilidad del equipo de soporte técnico durante la ejecución de la planificación, o solicitudes de mantenimientos preventivo y /o correctivo de los equipos de cómputo de la institución, para tener evidencias en casos de acciones disciplinarias, cierta clase de información debe capturarse, grabarse y guardarse cuando se sospeche que se esté llevando a cabo abuso, fraude u otra falta que involucre los sistemas informáticos. Para tal efecto deberá crearse un expediente del estado del ordenador por cada usuario.

Dominio: A.17: Aspectos de seguridad de la información de la gestión de continuidad de negocio.

Control: A.17.1: Continuidad de seguridad de la información.

a) Los expedientes del estado de los ordenadores por cada usuario que realiza el equipo de soporte técnico, los registros de auditoría (papeles de trabajo) que evidencian los eventos relevantes sobre la seguridad de los sistemas informáticos, deben revisarse periódicamente y guardarse durante un tiempo prudencial de por lo menos cuatro meses. Dichos archivos son importantes para la detección de intrusos, brechas en la seguridad, investigaciones, y otras actividades de auditoría. Por tal razón deben protegerse para que nadie los pueda alterar y que sólo los pueden leer las personas autorizadas, lo que permitirán la continuidad de la seguridad de la información.

Control: A.17.1.1: Planificación de la continuidad de la seguridad de la seguridad de la información.

a) El Comité de Seguridad de la Información, será el responsable de la coordinación del desarrollo de los procesos que garanticen la continuidad de la seguridad de la información de la institución.

b) Se establece la necesidad de contar con un Plan de Continuidad de las Actividades de la institución que contemple los siguientes puntos:

- Identificar los eventos (amenazas) que puedan ocasionar interrupciones en los procesos de las actividades.
- Evaluar los riesgos para determinar el impacto de dichas interrupciones, tanto en términos de magnitud de daño como del período de recuperación.
- Identificar los controles preventivos.

Control: A.17.1.2: Implementación de la continuidad de la seguridad de la seguridad de la información.

a) Los propietarios de la información y usuarios de recursos de información, con la asistencia del responsable de seguridad informática, elaborarán los planes de contingencia necesarios

para garantizar la continuidad de las actividades de la institución. Estos procesos deberán ser propuestos por el Comité de Seguridad de la Información.

b) Se mantendrá un solo marco para los planes de continuidad de las actividades de institución, a fin de garantizar que los mismos sean uniformes e identificar prioridades de prueba y mantenimiento.

c) Cada plan de continuidad especificará claramente las condiciones para su puesta en marcha, así como las personas a cargo de ejecutar cada componente del mismo.

Control: A.17.1.3: Verificación, revisión y evaluación de la continuidad de la seguridad de la seguridad de la información.

a) El Comité de Seguridad de la Información establecerá un cronograma de pruebas periódicas de cada uno de los planes de contingencia. Realizándose ensayos, mantenimientos y reevaluaciones de los planes de continuidad de la institución.

Control: A.18.2: Revisiones de seguridad de la información.

a) Cada responsable de unidad organizativa de la institución (directores de departamentos, responsable de contabilidad) velará por la correcta implementación y cumplimiento de las normas y procedimientos de seguridad establecidos, dentro de su área de responsabilidad.

b) El responsable de seguridad informática, realizará revisiones periódicas de todas las áreas de la institución a efectos de garantizar el cumplimiento del marco de referencia de seguridad de la información.

c) Los propietarios de la Información brindarán apoyo a la revisión periódica del cumplimiento del marco de referencia de seguridad de la información.

Control: A.18.2.1: Revisiones independientes de la seguridad de la información.

a) El responsable de seguridad informática, realizará revisiones a los controles del marco de referencia a intervalos planificados o cuando ocurran cambios significativos, para crear

nuevas propuestas las que serán evaluadas y aprobadas por el Comité de Seguridad de la Información.

11.4 Percepción de los usuarios acerca de la utilidad de la aplicación de un marco de referencia de seguridad de la información en el uso de los equipos de cómputo.

Para lograr el cuarto objetivo se realizó encuesta donde se refleja la percepción de los participantes de este estudio. Se encuestaron a los usuarios de los departamentos de: Ciencia tecnología y salud, empresariales y administrativas, educación y humanidades, también a las oficinas de pedagogía, matemática y contabilidad. (ver anexos: grado de satisfacción de usuarios claves).

Como resultado de la encuesta aplicada, se encontró que el 100% de los participantes creen importante la protección de la información confidencial de la institución. Además, el 100% también consideran que la creación de mecanismos para proteger la información de la institución es útil y necesaria. Así mismo, el 100% de ellos afirma que la institución debe contar con medidas de seguridad de sus servicios de cómputos, que garanticen la seguridad de sus datos confidenciales.

Por tanto, se puede inferir que los participantes de este estudio ven una necesidad real e inmediata de contar con mecanismos o un marco de referencias que garanticen la integridad, disponibilidad y confidencialidad de la información. Estas normativas o mecanismos disminuiran los riesgos y amenazas que los servicios de cómputos de la FAREM-Estelí enfrentan, como se planteó en la hipótesis de este estudio (ver hipótesis).

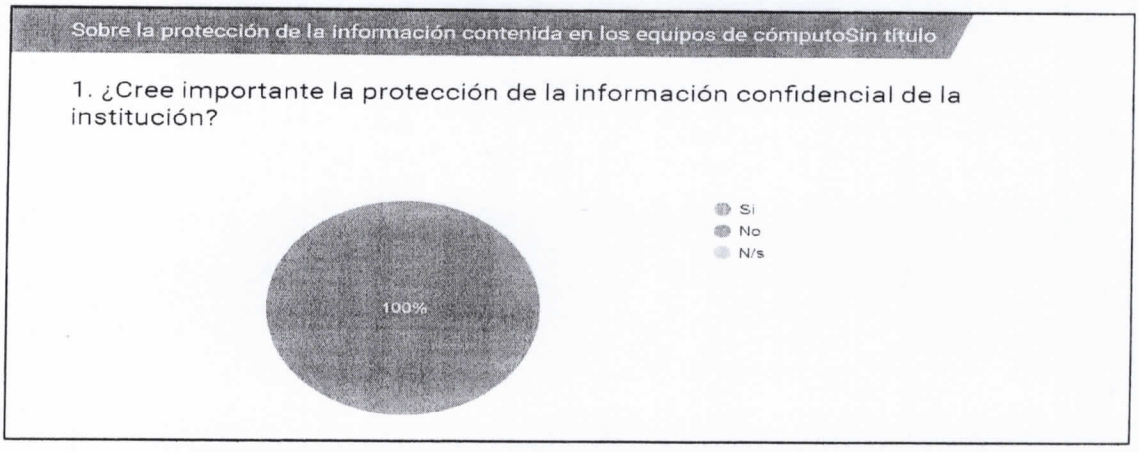


Figura No.1: Grado de satisfacción de usuarios claves sobre protección de información

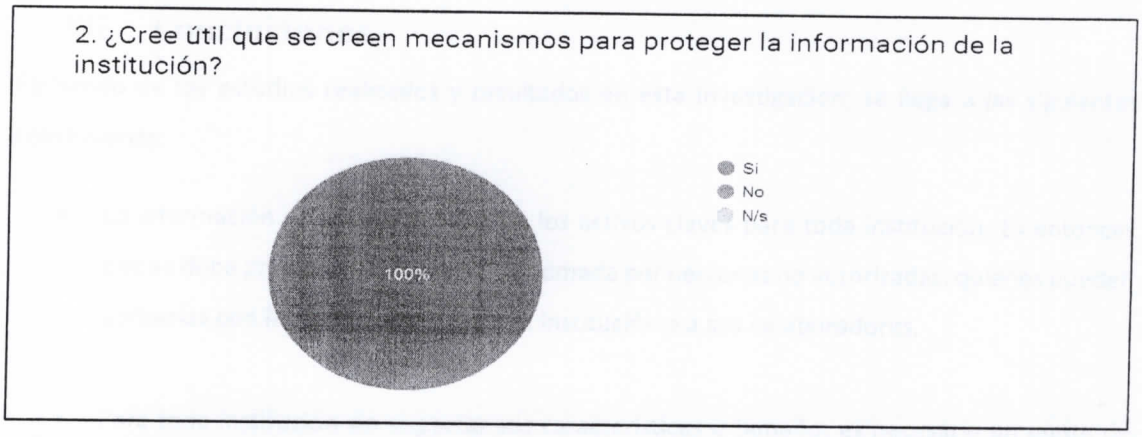


Figura No.2: Grado de satisfacción de usuarios claves sobre mecanismos de protección de información

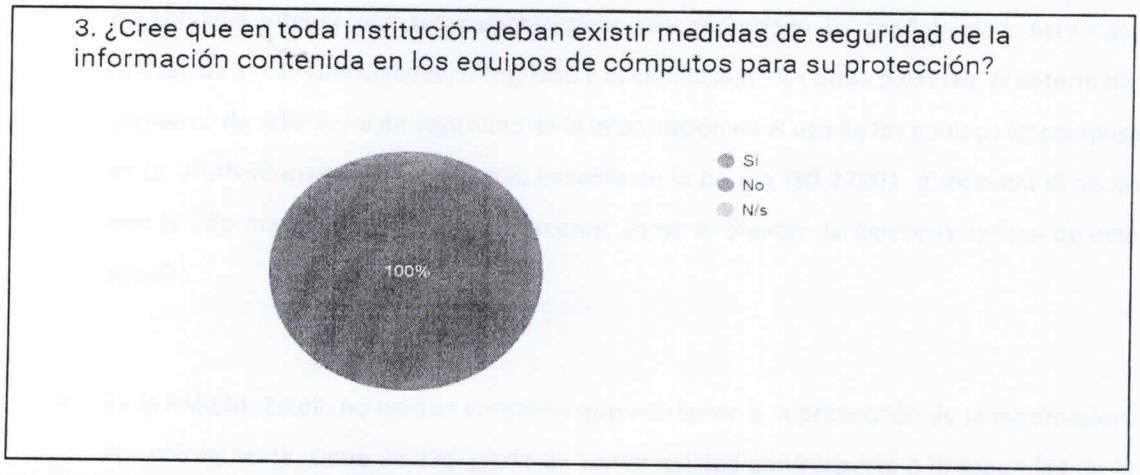


Figura No.3: Grado de satisfacción de usuarios claves sobre existencia de medidas de seguridad de información

XII. Conclusiones

Partiendo de los estudios realizados y resultados en esta investigación, se llega a las siguientes conclusiones:

- La información es hoy en día uno de los activos claves para toda institución. Es entonces que se debe proteger para que no sea tomada por personas no autorizadas, quienes pueden utilizarlas con fines de desprestigiar la institución o a sus colaboradores.

- Para toda institución sin importar sus características o tamaño, es necesario un punto de partida para la protección de la información confidencial de la institución y personal de los colaboradores, por considerarse ésta un activo de gran valía. La información debe conservarse íntegra con sus características que garanticen su confiabilidad. Esto hace referencia a: confidencialidad, integridad y disponibilidad. En otras palabras, el determinar un marco de referencia de seguridad de la información en el uso de los equipos de cómputo en la UNAN-Managua/FAREM-Estelí, basadas en la norma ISO 27001, disminuirá el riesgo que la información sea usada por terceros, como lo planteó la hipótesis central de este estudio.

- En la FAREM- Estelí, no existen controles que colaboren a la protección de la información. Por consiguiente, tiene un alto grado de vulnerabilidad con respecto a la seguridad de la información, toda institución está en la obligación de cuidar su imagen, prestigio y reputación es por eso que se ha iniciado con esta propuesta de un marco de referencia de seguridad de la información.

- Para la FAREM- Estelí, es urgente iniciar con un proceso de protección de la información para disminuir el nivel de riesgo de forma significativa y con ello la materialización de las amenazas y la reducción del impacto.

XIII. Recomendaciones

A continuación, se presentan algunos puntos importantes que se deben de tomar en cuenta para el fortalecimiento de la seguridad de la información contenida en los equipos de cómputos de la FAREM-Estelí.

- Establecer mecanismos que con precisión indiquen qué está permitido y qué no está permitido manipular en los ordenadores.

- Establecimiento inmediato de un marco de referencia de seguridad de la información y seguimiento de controles sobre ellas.

- Capacitar al personal de la FAREM-Estelí, en aspectos relacionados con seguridad de la información.

- Concienciar a todas las personas que integran esta importante facultad para aportar a fortalecer las iniciativas en pro de su buena andanza, para lo que deben empoderarse y conocer que la seguridad de la información se considera un sistema y se convierte en una actividad de gestión. La seguridad deja de ser un conjunto de actividades más o menos organizadas y pasa a transformarse en un ciclo de vida metódico y controlado, en el que participa toda la institución.

XIV. Bibliografía

Bonilla, J. de D. (2011). *Sistema de formación gerencial para el instituto nicaragüense de fomento cooperativo*. Tesis para optar al grado de Master en Computación, con énfasis en Sistemas de Información. UNAN-Managua.

Ríos, S. R. (2014). *Políticas para las tecnologías de la información (TIC) en la dirección de informática de la Asociación Pueblos en Acción Comunitaria Aplicando COBIT 4.1, en el año 2013*. Tesis para optar al grado de Master en Computación, con énfasis en Sistemas de Información. UNAN-Managua.

Carrasco, A. (2013). Conceptos de seguridad informática y su reflejo en la Cámara de Cuentas de Andalucía. *Auditoría Pública nº 61*, pp. 111-117.

ISO (International Standard Organization). (2011). *Gestión del riesgo – Principios directrices*. Estándar de Seguridad ISO 31000.

Diccionario de la Real Academia Española (2008). Información [en línea]. [Fecha de consulta: 06 de febrero 2015]. Disponible en http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=informaci%C3%B3n

Johnson, C. (2005). Los beneficios del PDCA. [recurso electrónico] [Fecha de consulta: 07 de febrero 2016]. Disponible en http://asq.org/quality-progress/2002/05/problem-solving/los-beneficios-de-pdca.html

Ramió, J. (2006). *Libro electrónico de seguridad informática y criptografía*. Versión 4.1 de 1 de marzo 2006.

Ramírez, A. & Ortiz, Z. (2011). Gestión de riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios. En: *Ingeniería, Vol. 16, No. 2*, pág. 56-66

Sampieri, R., Collado, C. & Lucio, P. (2010). *Metodología de la investigación*. (5ta Ed.). México DF: McGraw-Hill Interamericana

Piura, J. (1994). Introducción a la Metodología de la Investigación Científica, Nicaragua: El amanecer s.a.

Hernández, Fernández & Baptista. (2004). Metodología de la Investigación, México: Mc Graw Hill

XV. Compendio

Universidad Nacional Autónoma de Nicaragua
UNAN, Managua

ENCUESTA

Objetivo: Conocer si los usuarios finales de los equipos de cómputos de la FAREM-Estelí; tienen noción sobre seguridad informática en general y la exposición de la información en ellos contenida.

Seguridad General

1. Los ordenadores de su institución, ¿tienen instalado antivirus?

Sí No n/s

2. El antivirus que tienen instalado (si es el caso), ¿está actualizado con las últimas definiciones?

Sí No n/s

3. ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la institución?

Sí No n/s

4. ¿Se utilizan programas de descarga de archivos de usuario (música, películas, programas...)?

Sí No n/s

5. ¿Dispone de baterías (SAI) para cada ordenador, para evitar apagones y sobretensiones?

Sí No n/s

6. ¿Existen normativas de acceso a los equipos de cómputo?

Sí No n/s

7. ¿Existe acceso restringido a las áreas donde se encuentran las computadoras que ustedes usan para desempeñar sus labores en la institución?

Sí No n/s

8. ¿Los equipos de cómputos son multiusuarios?

Sí No n/s

9. Si la respuesta anterior es si, ¿Se cuenta con una cuenta y contraseña para cada usuario de manera obligatoria?

Sí No n/s

Datos de la institución

1. ¿Las computadoras de trabajo tienen datos de la institución almacenados dentro de su disco duro?

Sí No n/s

2. ¿Se realiza copia de seguridad de los datos de la institución?

Sí No n/s

3. En caso de que se realice copia de seguridad, con qué frecuencia

Diaria semanal otro

4. ¿Se realiza un mantenimiento de las copias de seguridad de la institución?

Sí No n/s

Programas y Aplicaciones Informáticas

1. ¿Existe algún encargado de instalar/desinstalar los programas y aplicaciones informáticas en su institución?

Sí No n/s

2. ¿Es permitido para cualquier usuario instalar programas en los ordenadores?

Sí No n/s

3. ¿Existen políticas de prohibición para que la instalación de programas solamente la realice el personal autorizado?

Sí No n/s

Sobre la protección de la información contenida en los equipos de cómputo

1. ¿Cree importante la protección de la información confidencial de la institución?
   Sí No n/s

2. ¿Cree útil que se creen mecanismos para proteger la información de la institución?
   Sí No n/s

3. ¿Cree que en toda institución deban existir medidas de seguridad de la información contenida en los equipos de cómputos para su protección?
   Sí No n/s

Universidad Nacional Autónoma de Nicaragua
UNAN, Managua

ENTREVISTA

Objetivo: Conocer el grado de seguridad aplicado por el personal de soporte técnico a los equipos de cómputo de la FAREM-Estelí; con relación al acceso de los usuarios finales.

Seguridad General

1. ¿Cuáles cree usted que son los beneficios de que los ordenadores dispongan de cuentas de usuarios y contraseñas?

2. ¿Está actualizado el antivirus que tiene instalado con las últimas definiciones? ¿Cómo cree usted que le afecta este hecho a usted?

3. ¿Se realiza un mantenimiento informático periódico sobre los ordenadores de la institución? ¿Quién y cuándo lo realiza?

4. ¿Están autorizados los usuarios de descargar y almacenar en sus discos duros música, películas, programas?

5. ¿Es permitido instalar programas sin autorización por parte de los usuarios finales de los ordenadores?

6. ¿Qué políticas existen que indiquen como deben establecerse, y con qué frecuencia de tiempo deben cambiarse las contraseñas?

7. ¿Existen políticas que restrinjan el acceso a personas ajenas a la institución a los equipos de cómputo? En caso positivo, ¿cuáles?

8. ¿Es permitido que las personas ajenas a los funcionarios de la institución accedan a las áreas donde se encuentran ubicadas las computadoras? Explique.

9. ¿Existen medidas por escrito para las computadoras multiusuarios? En caso positivo, ¿cuáles?

10. ¿Existen patrones para la creación de contraseñas en las computadoras que las poseen en el caso particular de que la usen varias personas? ¿En qué consisten éstos?

Datos de la institución

1. ¿Los equipos de cómputos de trabajo tienen datos de la institución almacenados dentro de su disco duro?

2. ¿Quién realiza copia de seguridad de los datos de la institución?

3. En caso de que se realice copia de seguridad, ¿con qué frecuencia se realiza?

4. ¿Se realiza un mantenimiento de las copias de seguridad de la institución?

Programas y Aplicaciones Informáticas

1. ¿Existe un encargado de instalar/desinstalar los programas y aplicaciones informáticas en su empresa? ¿Qué criterios se siguen al designar a ese técnico?

2. ¿Es permitido para cualquier usuario instalar programas en los ordenadores?

3. ¿Qué políticas existen de prohibición para que la instalación de programas solamente la realice el personal autorizado?

Sobre la protección de la información contenida en los equipos de cómputo

1. ¿Por qué considera usted importante la protección de la información confidencial de la institución?

2. ¿Cree útil que se creen mecanismos para proteger la información de la institución? Fundamente su respuesta.

3. ¿Por qué cree que en toda institución deban existir medidas de seguridad de la información contenida en los equipos de cómputos para su protección?

Universidad Nacional Autónoma de Nicaragua
UNAN, Managua

GUÍA DE OBSERVACIÓN

Objetivo: Conocer el estado actual de la seguridad de la información en los equipos de cómputo de la FAREM-Estelí; con relación al acceso de los usuarios finales.

ITEM	SI	NO	N/A
Presenta el equipo cuentas de usuarios			
Las cuentas de usuarios solicitan contraseña			
Las cuentas de usuarios están limitadas o restringidas			
Los equipos de cómputos tienen instalado antivirus			
Está actualizado el antivirus			
El usuario puede descargar y almacenar en su disco duro música, videos, películas.			
Los equipos de cómputos presentan estándar con respecto a los programas instalados.			
Los equipos de cómputo son usados por personas ajenas a los funcionarios de la institución.			
Los equipos de cómputos de trabajo contienen datos de la institución almacenados en su disco duro.			

Tabla No. 8: Guía de observación.

XVI. Anexos

Matriz de Análisis de Riesgo	Clasificación				Probabilidad de Amenaza [1 = Insignificante, 2 = Baja, 3= Mediana, 4 = Alta]																			
					Actos originados por la criminalidad común y motivación política													Sucesos de origen físico							
Datos e Información	Confidencial, Privado, Sensitivo	Obligación por ley / Contrato / Convenio	Costo de recuperación (tiempo, económico, material, imagen, emocional)	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Allanamiento (ilegal, legal)	Persecución (civil, fiscal, penal)	Orden de secuestro / Detención	Sabotaje (ataque físico y electrónico)	Daños por vandalismo	Extorsión	Fraude / Estafa	Robo / Hurto (físico)	Robo / Hurto de información electrónica	Intrusión a Red interna	Infiltración	Virus / Ejecución no autorizado de programas	Violación a derechos de autor	Incendio	Inundación / desiave	Sismo	Polvo	Falta de ventilación	Electromagnetismo	Sobrecarga eléctrica	Falta de corriente (apagones)
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)																								
Finanzas																								
Servicios bancarios																								
RR.HH																								
Directorio de Contactos																								
Productos institucionales (Investigaciones, Folletos, Fotos, etc.)																								

Figura No.4: Matriz del análisis de riesgos

Matriz de Análisis de Riesgo		Probabilidad de Amenaza					
Elementos de Información	Magnitud de Daño	Criminalidad		Sucesos físicos		Negligencia	
		Robo	Virus	Incendio	Falta de Corriente	Compartir contraseñas	No cifrar datos críticos
		3	4	2	3	4	3
Datos e Información							
RR.HH	3	9	12	6	9	12	9
Finanzas	4	12	16	8	12	16	12
Sistema e Información							
Computadoras	2	6	8	4	6	8	6
Portátiles	3	9	12	6	9	12	9
Personal							
Coordinador	4	12	16	8	12	16	12
Personal técnico	3	9	12	6	9	12	9

Figura No.5: Análisis de riesgos

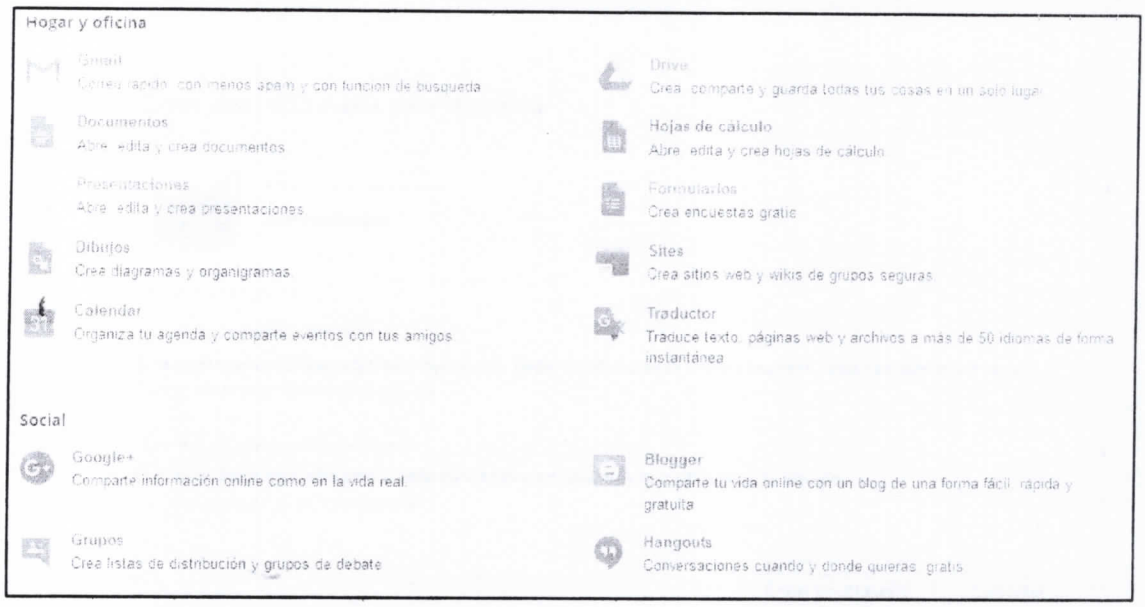


Figura No.6: Plataforma Formulario de Google

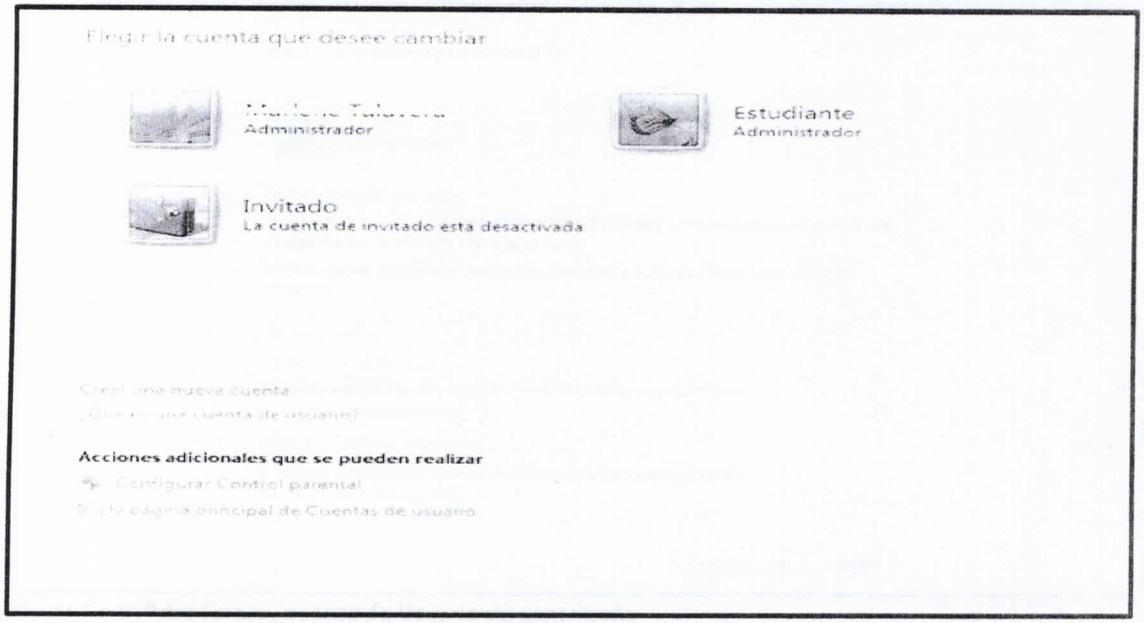


Figura No.7: Print Screen, la cuenta estudiante con privilegios de administrador

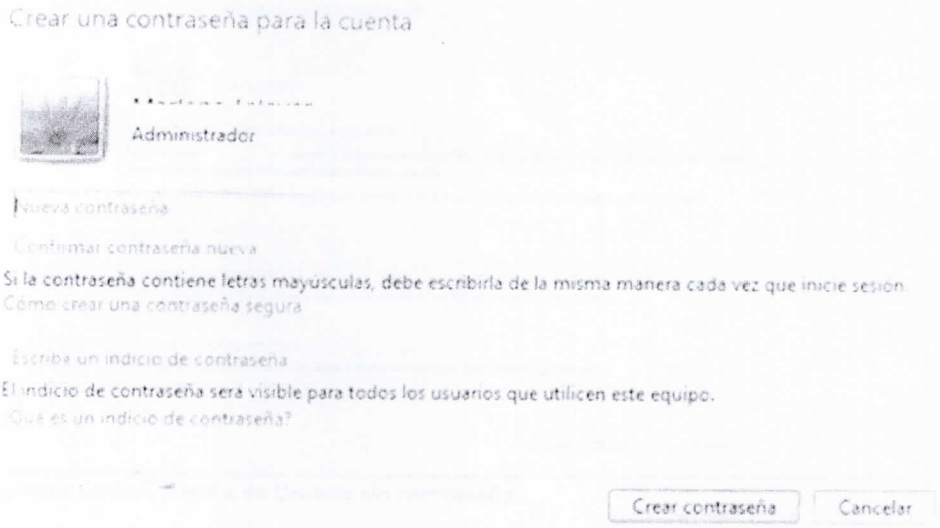


Figura No.8: Print Screen, cuenta de Administrador sin contraseña

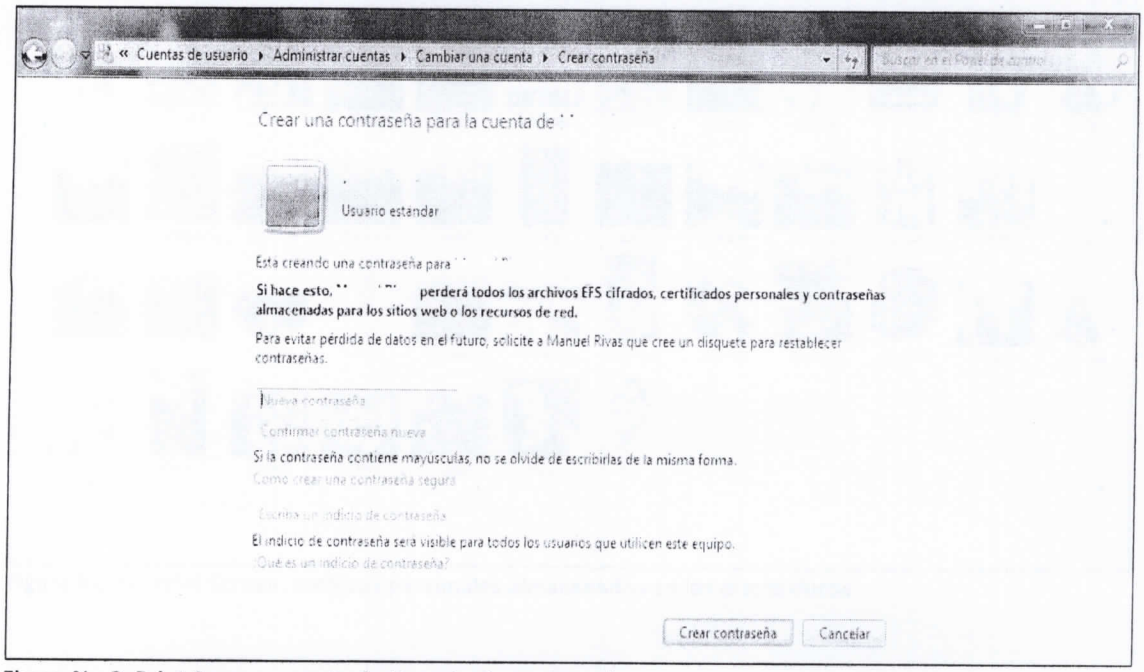


Figura No.9: Print Screen, cuenta de Usuario sin contraseña

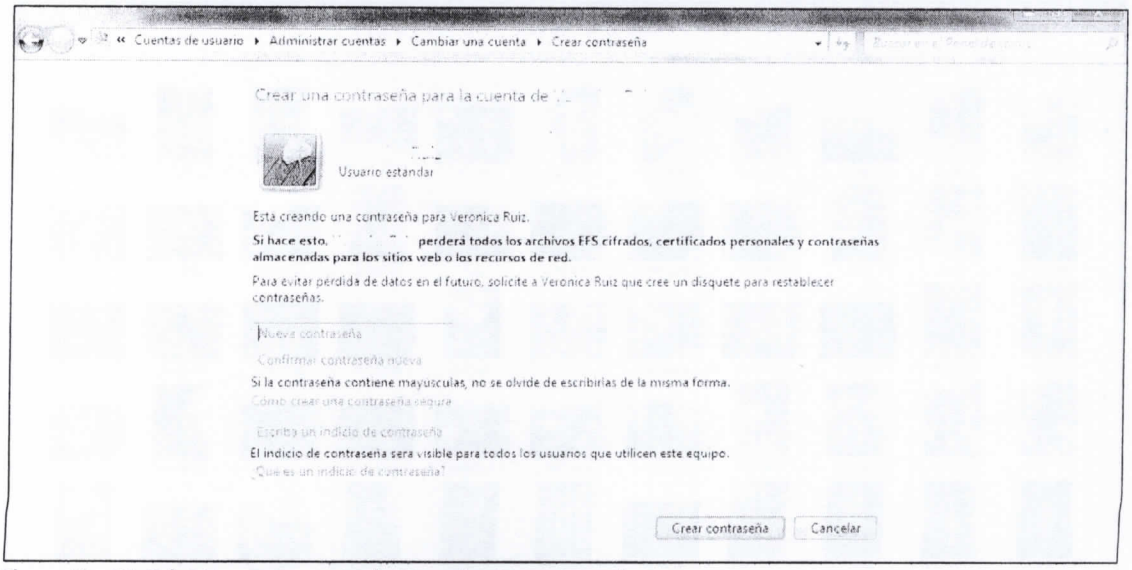


Figura No.10: Print Screen, cuenta de Usuario sin contraseña

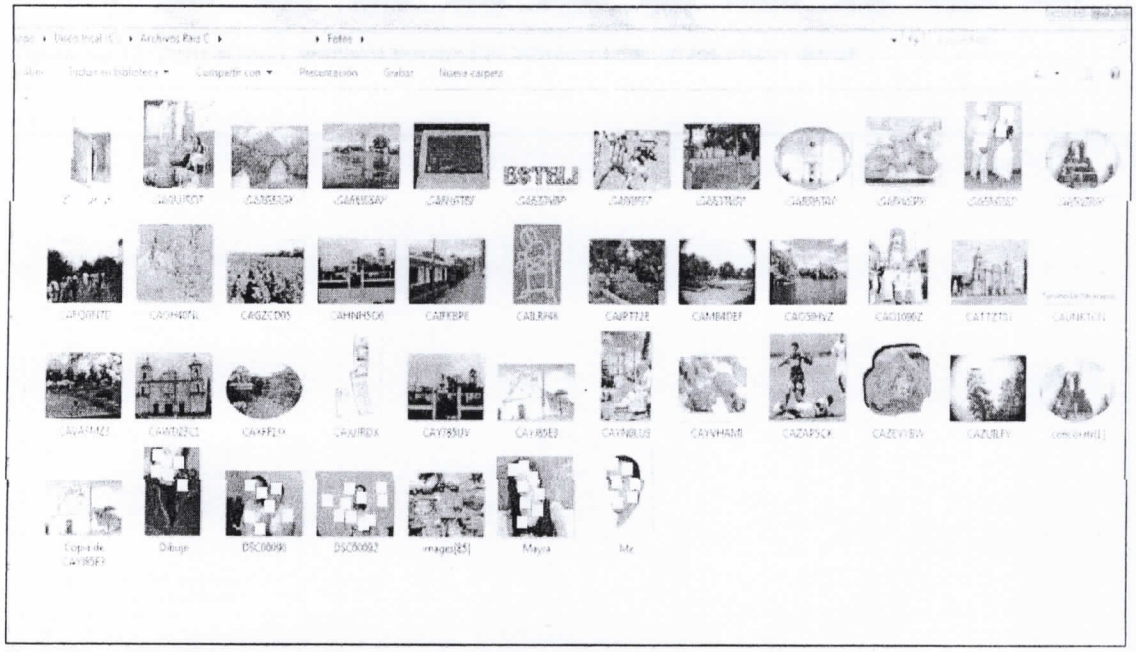


Figura No.11: Print Screen, archivos personales almacenados en los discos duros

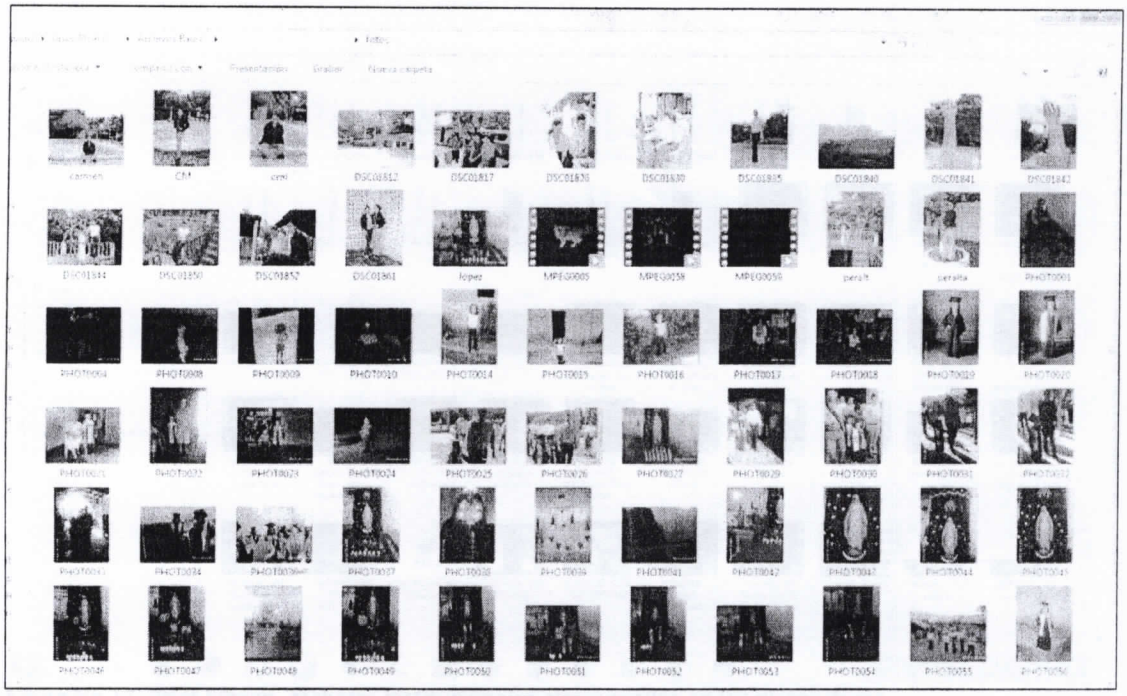


Figura No.12: Print Screen, archivos personales almacenados en los discos duros

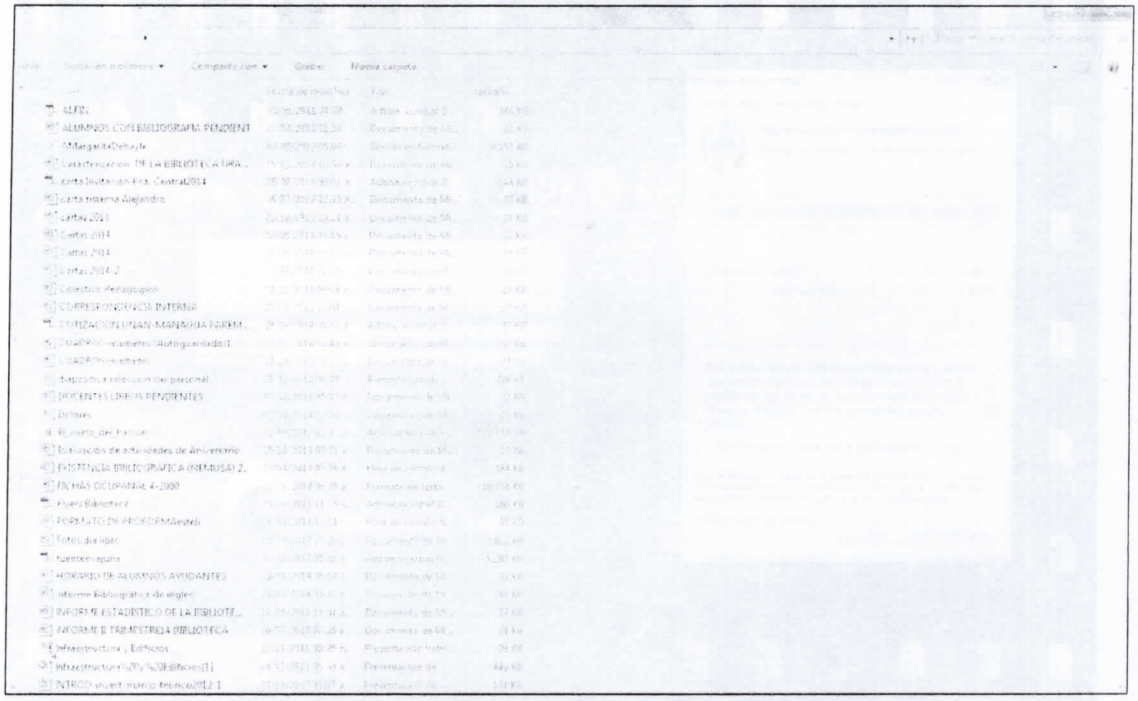


Figura No.13: Print Screen, archivos institucionales almacenados en los discos duros

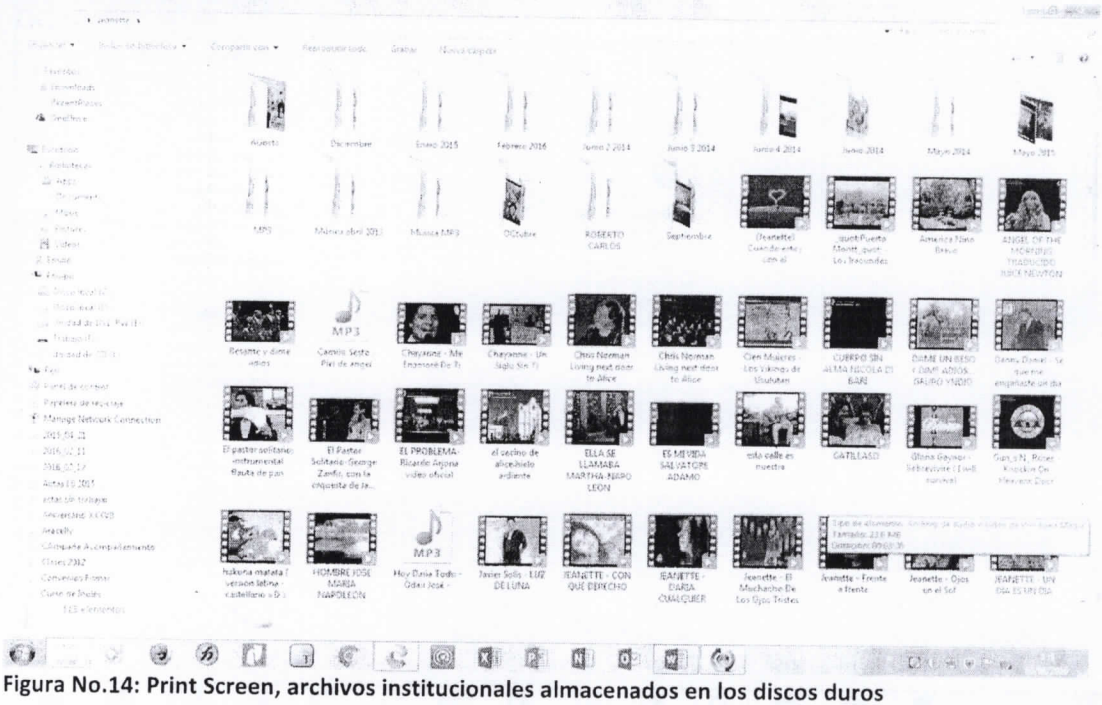


Figura No.14: Print Screen, archivos institucionales almacenados en los discos duros

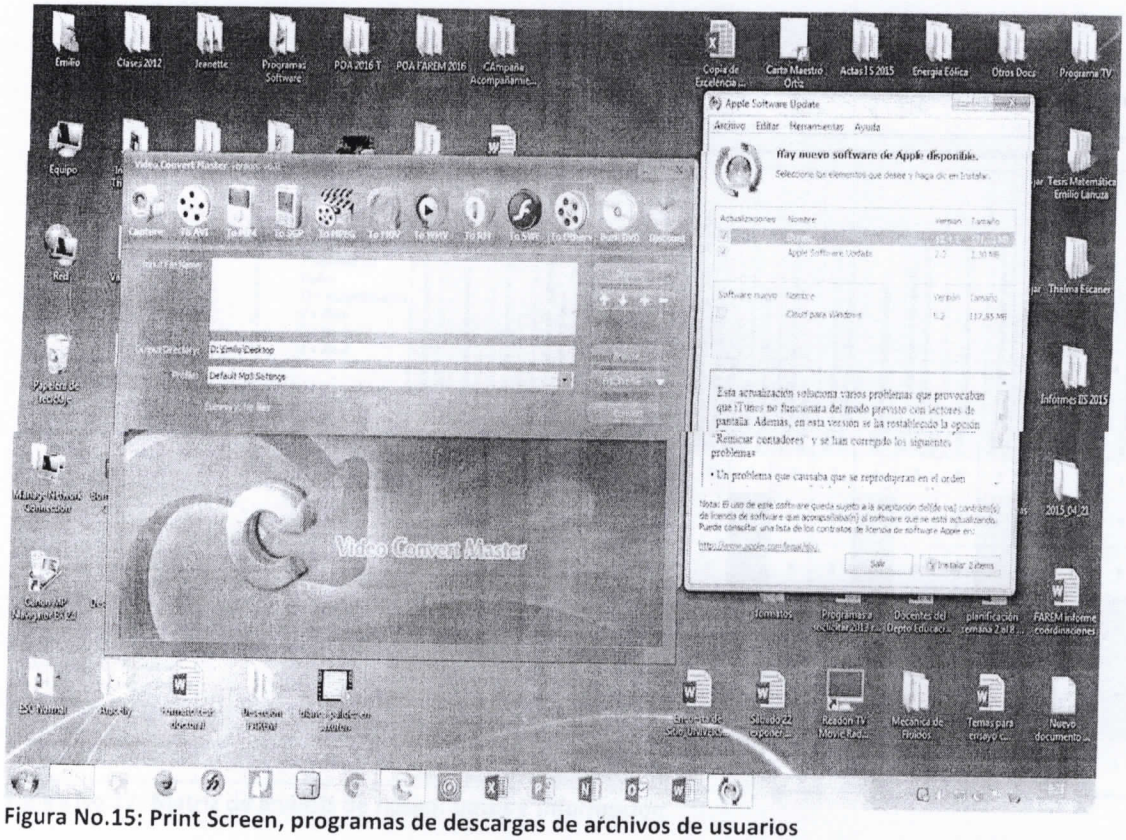


Figura No.15: Print Screen, programas de descargas de archivos de usuarios

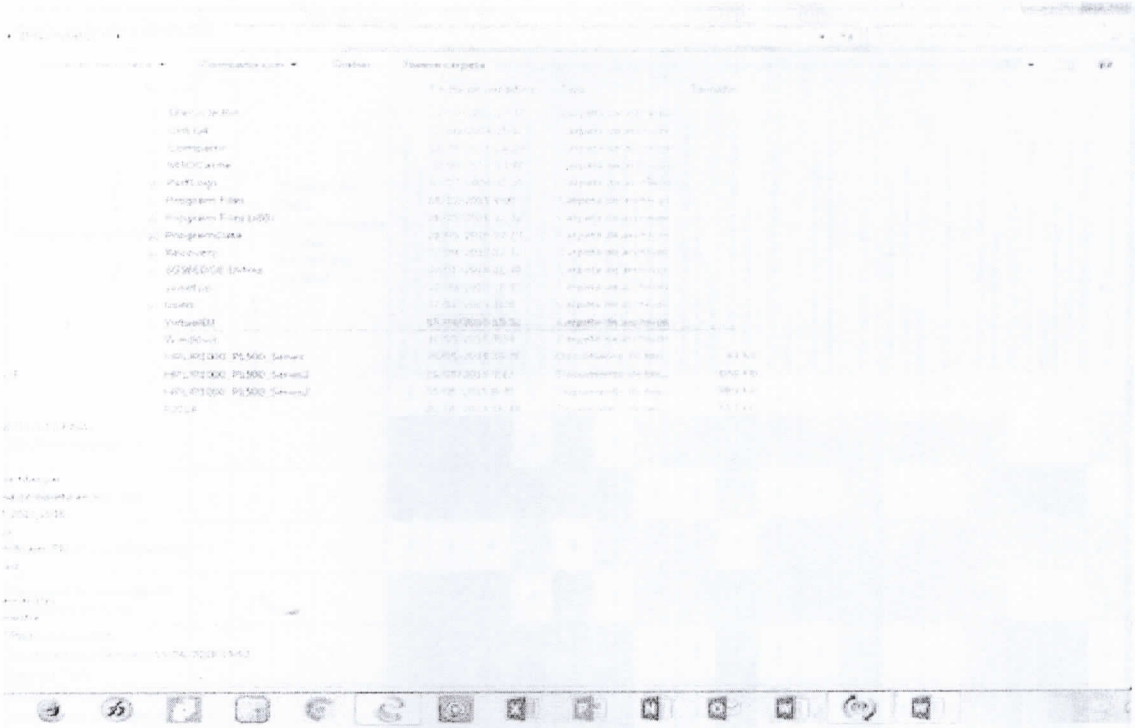


Figura No.16: Print Screen, programas de descargas de archivos de usuarios

Matriz de Análisis de Riesgo			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																		
Datos e Información	Clasificación: Confidencial, Privado, Sensitivo	Magnitud de Daño: (1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto)	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a traves de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.;	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas.)	Compartir contraseñas o permisos a terceros no autorizados	Transmision de contraseñas por telefono	Exposición o extravio de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de actualizacion de software	Fallas en permisos de usuarios (acceso a archivos.)	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificacion de normas y reglas / Análisis inadecuado de datos de	Ausencia de documentación
			4	4	4	3	4	3	2	2	4	2	2	1	2	2	1	3	3	2
Documentos institucionales (Proyectos, Planes, Evaluaciones, Informes, etc.)	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8
Documentos personales (Cartas, gestiones, etc)	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8
Ausencia de copia de seguridad de los datos de la institución	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Ausencia de mantenimiento de las copias de seguridad de la institución	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Acceso a sistemas propios de la institución	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8

Figura No.17: Matriz de análisis de riesgo: Datos e Información

Matriz de Análisis de Riesgo	Clasificación			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																
Sistemas e Infraestructura	Acceso exclusivo	Acceso ilimitado	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravió de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de	Ausencia de documentación
				4	4	4	3	4	3	2	2	4	2	2	1	2	2	1	3	3	2
Anti Virus Instalado	x	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Anti Virus Actualizado	x	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8
Mantenimiento a Ordenadores	x	x	2	8	8	8	6	8	6	4	4	8	4	4	2	4	4	2	6	6	4
Programas de descargas de archivos de usuarios	x	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Protección contra fluctuaciones eléctricas baterías (SAI)	x	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8
Equipos de cómputos son multiusuarios sin control de acceso	x	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8

Figura No.18: Matriz de análisis de riesgo: Sistemas e Infraestructura

Matriz de Análisis de Riesgo	Clasificación			Sucesos derivados de la impericia, negligencia de usuarios/as y decisiones institucionales																
Personal	Acceso Exclusivo	Acceso Ilimitado	Magnitud de Daño: [1 = Insignificante 2 = Bajo 3 = Mediano 4 = Alto]	Falta de inducción, capacitación y sensibilización sobre riesgos	Mal manejo de sistemas y herramientas	Utilización de programas no autorizados	Falta de pruebas de software nuevo con datos productivos	Perdida de datos	Infección de sistemas a través de unidades portables sin escaneo	Manejo inadecuado de datos críticos (codificar, borrar, etc.)	Manejo inadecuado de contraseñas (inseguras, no cambiar, compartidas)	Compartir contraseñas o permisos a terceros no autorizados	Transmisión de contraseñas por teléfono	Exposición o extravió de equipo, unidades de almacenamiento, etc	Sobrepasar autoridades	Falta de definición de perfil, privilegios y restricciones del personal	Falta de actualización de software	Fallas en permisos de usuarios (acceso a archivos)	Falta de normas y reglas claras (no institucionalizar el estudio de los riesgos)	Falta de mecanismos de verificación de normas y reglas / Análisis inadecuado de datos de	Ausencia de documentación
				4	4	4	3	4	3	2	2	4	2	2	1	2	2	1	3	3	2
Ausencia normativas de acceso a los equipos de cómputo	x		3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Ausenciade acceso restringido a las áreas donde se encuentran las computadoras	x	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Ausencia de una cuenta y contraseña para cada usuario	x	x	4	16	16	16	12	16	12	8	8	16	8	8	4	8	8	4	12	12	8
Equipo técnico es el encargado de instalar/desinstalar los programas y aplicaciones informáticas en su institución	x	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6
Cualquier usuario instalar programas en los ordenadores	x	x	3	12	12	12	9	12	9	6	6	12	6	6	3	6	6	3	9	9	6

Figura No.19: Matriz de análisis de riesgo: Personal

16.1 Matriz para el Análisis de Riesgo

La Matriz para el Análisis de Riesgo, es producto del proyecto de Seguimiento al "Taller Centroamericano Ampliando la Libertad de Expresión: Herramientas para la colaboración, información y comunicación seguras" y fue punto clave en analizar y determinar los riesgos en el manejo de los datos e información de las organizaciones sociales participantes. La Matriz, se basa en una hoja de cálculo, no dará un resultado detallado sobre los riesgos y peligros de cada recurso (elemento de información) de la institución, sino una mirada aproximada y generalizada de estos.

Hay que tomar en cuenta que el análisis de riesgo detallado, es un trabajo muy extenso y consumidor de tiempo, porque requiere que se compruebe todos los posibles daños de cada recurso de una institución contra todas las posibles amenazas, es decir terminaríamos con un sinnúmero de grafos de riesgo que deberíamos analizar y clasificar.

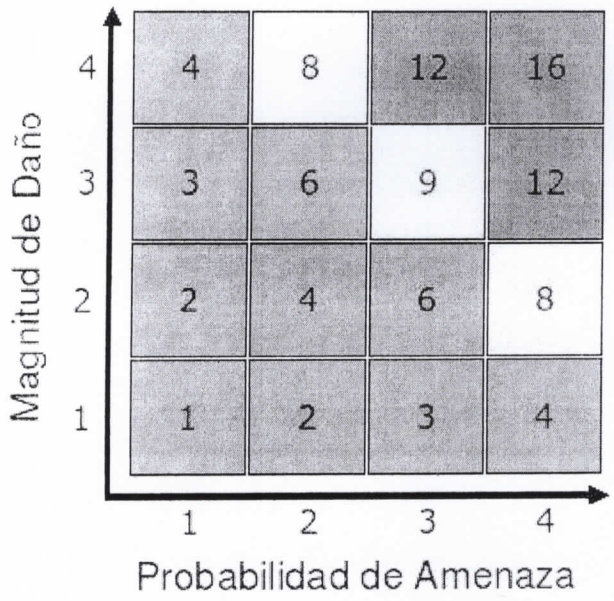
Entonces lo que se pretende con el enfoque de la Matriz es localizar y visualizar los recursos de una organización, que están más en peligro de sufrir un daño por algún impacto negativo, para posteriormente ser capaz de tomar las decisiones y medidas adecuadas para la superación de las vulnerabilidades y la reducción de las amenazas.

16.1.1 Fundamento de la Matriz

La Matriz se basa en el método de Análisis de Riesgo con un grafo de riesgo, usando la formula Riesgo = Probabilidad de Amenaza x Magnitud de Daño

La Probabilidad de Amenaza y Magnitud de Daño pueden tomar los valores y condiciones respectivamente.

1 = Insignificante (incluido Ninguna)
2 = Baja
3 = Mediana
4 = Alta



El Riesgo, que es el producto de la multiplicación Probabilidad de Amenaza por Magnitud de Daño, está agrupado en tres rangos, y para su mejor visualización, se aplica diferentes colores.

- Bajo Riesgo = 1 – 6 (verde)
- Medio Riesgo = 8 – 9 (amarillo)
- Alto Riesgo = 12 – 16 (rojo)

Dependiendo del color de cada celda, podemos sacar conclusiones no solo sobre el nivel de riesgo que corre cada elemento de información de sufrir un daño significativo, causado por una amenaza, sino también sobre las medidas de protección necesarias.